Nortel Business Secure Router 222 Configuration — Basics

BSR222

Business Secure Router

Document Number: **NN47922-500**

Document Version: **1.4**

Date: **May 2007**

NORTEL

Copyright © Nortel 2005–2006

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. The information in this document is proprietary to Nortel.

Trademarks

Nortel, Nortel (Logo), the Globemark, and This is the way, This is Nortel (Design mark) are trademarks of Nortel.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Preface 29

Before you begin 29
Text conventions 29
Related publications 30
Hard copy technical manuals 30
How to get Help 31
Getting Help from the Nortel Web site 31
Getting Help over the phone from a Nortel Solutions Center 31
Getting Help from a specialist by using an Express Routing Code 32
Getting Help through a Nortel distributor or reseller 32

Chapter 1
Getting to know your Nortel Business Secure Router 222 33

Introducing the Nortel Business Secure Router 222 33
Features 33
Physical features 34
4-Port switch 34
Autonegotiating 10/100 Mb/s Ethernet LAN 34
Autosensing 10/100 Mb/s Ethernet LAN 34
Autonegotiating 10/100 Mb/s Ethernet WAN 34
Auxiliary port 35
Time and date 35
Reset button 35
Nonphysical features 35
IPSec VPN capability 35
Nortel Contivity Client Termination 35
Certificates 36
SSH 36

HTTPS 36
IEEE 802.1x for network security 36
Firewall 36
Brute force password guessing protection 37
Content filtering 37
Packet filtering 37
Universal Plug and Play (UPnP) 37
Call scheduling 37
PPPoE 37
PPTP Encapsulation 38
Dynamic DNS support 38
IP Multicast 38
IP Alias 38
Central Network Management 38
SNMP 39
Network Address Translation (NAT) 39
Traffic Redirect 39
Port Forwarding 39
DHCP (Dynamic Host Configuration Protocol) 39
Full network management 40
Road Runner support 40
Logging and tracing 40
Upgrade Business Secure Router Firmware 40
Embedded FTP and TFTP Servers 40
Applications for the Nortel Business Secure Router 222 41
Secure broadband internet access and VPN 41
Hardware Setup 42

Chapter 2
Introducing the WebGUI 43

WebGUI overview 43
Accessing the Business Secure Router WebGUI 43
Restoring the factory default configuration settings 46
Procedure to use the reset button 46
Uploading a configuration file via console port 46

Navigating the Business Secure Router WebGUI 47

Chapter 3
Wizard setup. 51

Wizard overview 51
Wizard setup: General Setup and System Name 51
Domain Name 52
Wizard setup: Screen 2 52
Ethernet 53
PPTP 54
PPPoE Encapsulation 56
Wizard setup: Screen 3 58
WAN IP address assignment 58
IP address and Subnet Mask 59
DNS Server address assignment 60
WAN MAC address 60
Basic Setup Complete 65

Chapter 4
User Notes 67

General Notes 67
General 67
Firewall 68
NAT 68
VPN Client Termination 69
Security 70
Routing 70
Advanced Router Configuration 71
Setting up the router when the system has a server 71
Connecting two sites to establish a virtual private network 71
Adding IP telephony to a multi-site network 72
Configuring the router to act as a Nortel VPN Server (Client Termination) . . . 73
Configuring the router to connect to a Nortel VPN Server (Client Emulation) . 73
Allowing remote management of a LAN-connected BCM50 74
Setting up the router for guest access 74

Preventing heavy data traffic from impacting telephone calls 75
Setting Up a Remote Office with a UNIStim IP Telephone 75
Inter-Operability With Third-Party Routers 76
VPN Connections With Cisco Routers 76

Chapter 5
System screens 77

System overview 77
DNS overview 77
Private DNS server 77
Configuring General Setup 78
Dynamic DNS 81
DYNDNS Wildcard 81
Configuring Dynamic DNS 81
Configuring Password 83
Predefined NTP time server list 85
Configuring Time and Date 86
ALG 90
Configuring ALG 90

Chapter 6
LAN screens 93

LAN overview 93
DHCP setup 93
IP pool setup 93
DNS servers 94
LAN TCP/IP 94
Factory LAN defaults 94
RIP setup 94
Multicast 95
Configuring IP 96
Configuring Static DHCP 100
Configuring IP Alias 101

Chapter 7
WAN screens 105

WAN Overview 105
TCP/IP Priority (Metric) 105
Configuring Route 106
Configuring WAN ISP 107
Ethernet Encapsulation 107
PPPoE Encapsulation 108
PPTP Encapsulation 110
Service type 112
Configuring WAN IP 114
Configuring WAN MAC 118
Traffic redirect 119
Configuring Traffic Redirect 120
Configuring Dial Backup 122
Advanced Modem Setup 127
AT Command Strings 127
DTR Signal 127
Response Strings 127
Configuring Advanced Modem Setup 128

Chapter 8
Network Address Translation (NAT) Screens 131

NAT overview 131
NAT definitions 131
What NAT does 132
How NAT works 133
Port Restricted Cone NAT 133
NAT application 134
NAT mapping types 135
Using NAT 136
SUA (Single User Account) versus NAT 136
SUA Server 137
Default server IP address 137
Port forwarding: Services and Port Numbers 138

Configuring servers behind SUA (example) 138
Configuring SUA Server 139
Configuring Address Mapping 141
Trigger Port Forwarding 145
Trigger Port Forwarding example 145
Two points to remember about Trigger Ports 146
Configuring Trigger Port Forwarding 147

Chapter 9
Static Route screens 149

Static Route overview 149
Configuring IP Static Route 150
Configuring Route entry 152

Chapter 10
Firewalls 155

Firewall overview 155
Types of firewalls 155
Packet Filtering firewalls 156
Application level firewalls 156
Stateful Inspection firewalls 156
Introduction to the Business Secure Router firewall 157
Denial of Service 158
Basics 158
Types of DoS attacks 159
Stateful inspection 163
Stateful inspection process 164
Stateful inspection and the Business Secure Router 165
TCP security 166
UDP/ICMP security 167
Upper layer protocols 167
Guidelines for enhancing security with your firewall 168
Packet filtering vs. firewall 169
Packet filtering: 169
When to use filtering 169

Firewall 169
When to use the firewall 170

Chapter 11
Firewall screens 171

Access methods 171
Firewall policies overview 171
Rule logic overview 173
Rule checklist 173
Security ramifications 173
Key fields for configuring rules 174
Action 174
Service 174
Source address 174
Destination address 174
Connection direction examples 174
LAN to WAN rules 175
WAN to LAN rules 175
Configuring firewall 176
Configuring firewall rules 180
Configuring source and destination addresses 183
Configuring custom ports 184
Example firewall rule 185
Predefined services 188
Alerts 191
Configuring attack alert 192
Threshold values 192
Half-open sessions 192
TCP maximum incomplete and blocking period 193

Chapter 12
Content filtering 197

Introduction to content filtering 197
Restrict web features 197
Days and Times 197

Configure Content Filtering 198

Chapter 13
VPN 201

VPN 201
IPSec 201
Nortel Business Secure Router 222 VPN functions 201
VPN screens overview 202
Other terminology 203
Encryption 203
Data confidentiality 204
Data integrity 204
Data origin authentication 204
VPN applications 204
IPSec architecture 204
IPSec algorithms 205
AH (Authentication Header) protocol 206
ESP (Encapsulating Security Payload) protocol 206
Key management 207
Encapsulation 208
Transport mode 208
Tunnel mode 208
IPSec and NAT 209
Secure Gateway Address 210
Dynamic Secure Gateway Address 211
Summary screen 211
Keep Alive 214
Nailed Up 214
NAT Traversal 215
NAT Traversal configuration 216
Preshared key 216
Configuring Contivity Client VPN Rule Setup 216
Configuring Advanced Setup 218
ID Type and content 220
ID type and content examples 221

My IP Address 222
Configuring Branch Office VPN Rule Setup 222
Configuring an IP Policy 231
Port forwarding server 236
Configuring a port forwarding server 236
IKE phases 238
Negotiation Mode 239
Preshared key 240
Diffie-Hellman (DH) Key Groups 240
Perfect Forward Secrecy (PFS) 240
Configuring advanced Branch office setup 241
SA Monitor 244
Global settings 246
VPN Client Termination 248
VPN Client Termination IP pool summary 252
VPN Client Termination IP pool edit 254
VPN Client Termination advanced 255

Chapter 14
Certificates 261

Certificates overview 261
Advantages of certificates 262
Self-signed certificates 262
Configuration summary 263
My Certificates 263
Certificate file formats 266
Importing a certificate 267
Creating a certificate 269
My Certificate details 272
Trusted CAs 276
Importing a Trusted CA's certificate 279
Trusted CA Certificate details 280
Trusted remote hosts 284
Verifying a certificate of a trusted remote host 286
Trusted remote host certificate fingerprints 286

Importing a certificate of a trusted remote host 288
Trusted remote host certificate details 289
Directory servers 293
Add or edit a directory server 294

Chapter 15
Bandwidth management 297

Bandwidth management overview 297
Bandwidth classes and filters 298
Proportional bandwidth allocation 298
Application based bandwidth management 298
Subnet based bandwidth management 298
Application and subnet based bandwidth management 299
Reserving bandwidth for nonbandwidth class traffic 299
Configuring summary 300
Configuring class setup 301
Bandwidth Manager Class Configuration 303
Bandwidth management statistics 306
Monitor 308

Chapter 16
IEEE 802.1x 309

IEEE 802.1x overview 309
RADIUS 309
Types of RADIUS messages 309
EAP Authentication overview 310
Configuring 802.1X 311

Chapter 17
Authentication server 315

Introduction to Local User database 315
Local User database 315
Edit Local User Database 317
Current split networks 320
Current split networks edit 321

Configuring RADIUS 323

Chapter 18
Remote management screens 327

Remote management overview 327
Remote management limitations 327
Remote management and NAT 328
System timeout 328
Introduction to HTTPS 329
Configuring WWW 330
HTTPS example 332
Internet Explorer warning messages 333
Netscape Navigator warning messages 333
Avoiding the browser warning messages 335
Logon screen 336
SSH overview 341
How SSH works 342
SSH implementation on the Business Secure Router 343
Requirements for using SSH 343
Configuring SSH 343
Secure Telnet using SSH examples 345
Example 1: Microsoft Windows 345
Example 2: Linux 346
Secure FTP using SSH example 347
Telnet 348
Configuring TELNET 349
Configuring FTP 350
Configuring SNMP 351
Supported MIBs 353
SNMP Traps 353
REMOTE MANAGEMENT: SNMP 354
Configuring DNS 355
Configuring Security 356

Chapter 19
UPnP 359

Universal Plug and Play overview 359
How do I know if I am using UPnP? 359
NAT Traversal 359
Cautions with UPnP 360
UPnP implementation 360
Configuring UPnP 360
Displaying UPnP port mapping 362
Installing UPnP in Windows example 363
Installing UPnP in Windows Me 363
Installing UPnP in Windows XP 364
Using UPnP in Windows XP example 366
Autodiscover Your UPnP-enabled Network Device 366
WebGUI easy access 369

Chapter 20
Logs Screens 371

Configuring View Log 371
Configuring Log settings 373
Configuring Reports 376
Viewing Web site hits 378
Viewing Protocol/Port 380
Viewing LAN IP address 381
Reports specifications 383

Chapter 21
Call scheduling screens 385

Call scheduling introduction 385
Call schedule summary 385
Call scheduling edit 387
Applying Schedule Sets to a remote node 389

Chapter 22
Maintenance 391

Maintenance overview 391
Status screen 391
System statistics 393
DHCP Table screen 394
F/W Upload screen 395
Configuration screen 398
Back to Factory Defaults 398
Backup configuration 399
Restore configuration 400
Restart screen 401

Appendix A
Troubleshooting 403

Problems Starting Up the Business Secure Router 403
Problems with the LAN LED 404
Problems with the LAN interface 404
Problems with the WAN interface 405
Problems with Internet Access 405
Problems accessing an internet Web site 406
Problems with the password 406
Problems with the WebGUI 407
Problems with Remote Management 407
Allowing Pop-up Windows, JavaScript and Java Permissions 408
Internet Explorer Pop-up Blockers 408
Allowing Pop-ups 408
Enabling Pop-up Blockers with Exceptions 409
Internet Explorer JavaScript 411
Internet Explorer Java Permissions 413
JAVA (Sun) 414
Netscape Pop-up Blockers 415
Allowing Pop-ups 416
Enable Pop-up Blockers with Exceptions 417
Netscape Java Permissions and JavaScript 419

Appendix B
Log Descriptions 423

VPN/IPSec Logs 432
VPN Responder IPSec Log 433
Log Commands 442
Configuring what you want the Business Secure Router to log 442
Displaying Logs 443
Log Command Example 444
Index 445

Figures

Figure 1 Secure Internet Access and VPN Application 41
Figure 2 Login screen 44
Figure 3 Change password screen 45
Figure 4 Replace certificate screen 45
Figure 5 Example Xmodem Upload 47
Figure 6 MAIN MENU Screen 48
Figure 7 Contact Support 49
Figure 8 Wizard 1 52
Figure 9 Wizard 2: Ethernet Encapsulation 53
Figure 10 Wizard 2: PPTP Encapsulation 55
Figure 11 Wizard2: PPPoE Encapsulation 57
Figure 12 Wizard 3 62
Figure 13 Private DNS server example 78
Figure 14 System general setup 79
Figure 15 DDNS 82
Figure 16 Password 84
Figure 17 Time and Date 87
Figure 18 ALG 90
Figure 19 LAN IP 96
Figure 20 Static DHCP 100
Figure 21 IP Alias 102
Figure 22 WAN: Route 106
Figure 23 Ethernet Encapsulation 107
Figure 24 PPPoE Encapsulation 109
Figure 25 PPTP Encapsulation 111
Figure 26 RR Service type 113
Figure 27 WAN: IP 115
Figure 28 MAC Setup 118
Figure 29 Traffic Redirect WAN Setup 119

Figure 30 Traffic Redirect LAN Setup 120
Figure 31 Traffic Redirect 121
Figure 32 Dial Backup Setup 123
Figure 33 Advanced Setup 128
Figure 34 How NAT works 133
Figure 35 Port Restricted Cone NAT 134
Figure 36 NAT application with IP Alias 135
Figure 37 Multiple servers behind NAT example 139
Figure 38 SUA/NAT setup 140
Figure 39 Address Mapping 142
Figure 40 Address Mapping edit 144
Figure 41 Trigger Port Forwarding process: example 146
Figure 42 Trigger Port 147
Figure 43 Example of Static Routing topology 150
Figure 44 Static Route screen 151
Figure 45 Edit IP Static Route 152
Figure 46 Business Secure Router firewall application 158
Figure 47 Three-way handshake 160
Figure 48 SYN flood 161
Figure 49 Smurf attack 162
Figure 50 Stateful inspection 164
Figure 51 LAN to WAN traffic 175
Figure 52 WAN to LAN traffic 176
Figure 53 Enabling the firewall 178
Figure 54 Creating and editing a firewall rule 181
Figure 55 Adding or editing source and destination addresses 183
Figure 56 Creating or editing a custom port 184
Figure 57 Firewall edit rule screen example 185
Figure 58 Firewall rule edit IP example 186
Figure 59 Edit custom port example 186
Figure 60 MyService rule configuration example 187
Figure 61 My Service example rule summary 188
Figure 62 Attack alert 194
Figure 63 Content filter 198
Figure 64 Encryption and decryption 203

Figure 65 IPSec architecture 205
Figure 66 Transport and Tunnel mode IPSec encapsulation 208
Figure 67 IPSec summary fields 211
Figure 68 Summary 212
Figure 69 NAT router between VPN switches 215
Figure 70 VPN Contivity Client rule setup 217
Figure 71 VPN Contivity Client advanced rule setup 218
Figure 72 VPN Branch Office rule setup 223
Figure 73 VPN Branch Office — IP Policy 231
Figure 74 VPN Branch Office — IP Policy - Port Forwarding Server 237
Figure 75 Two phases to set up the IPSec SA 238
Figure 76 VPN Branch Office advanced rule setup 241
Figure 77 VPN SA Monitor 245
Figure 78 VPN Global Setting 247
Figure 79 VPN Client Termination 249
Figure 80 VPN Client Termination IP pool summary 253
Figure 81 VPN Client Termination IP pool edit 254
Figure 82 VPN Client Termination advanced 256
Figure 83 Certificate configuration overview 263
Figure 84 My Certificates 264
Figure 85 My Certificate Import 268
Figure 86 My Certificate create 269
Figure 87 My Certificate details 273
Figure 88 Trusted CAs 277
Figure 89 Trusted CA import 279
Figure 90 Trusted CA details 281
Figure 91 Trusted remote hosts 285
Figure 92 Remote host certificates 287
Figure 93 Certificate details 287
Figure 94 Trusted remote host import 288
Figure 95 Trusted remote host details 290
Figure 96 Directory servers 293
Figure 97 Directory server add 295
Figure 98 Subnet based bandwidth management example 299
Figure 99 Bandwidth Manager: Summary 300

Figure 100 Bandwidth Manager: Class setup 302
Figure 101 Bandwidth Manager: Edit class 304
Figure 102 Bandwidth management statistics 307
Figure 103 Bandwidth manager monitor 308
Figure 104 EAP Authentication 311
Figure 105 802.1X 312
Figure 106 Local User database 316
Figure 107 Local User database edit 318
Figure 108 Current split networks 320
Figure 109 Current split networks edit 322
Figure 110 RADIUS 324
Figure 111 HTTPS implementation 330
Figure 112 WWW 331
Figure 113 Security Alert dialog box (Internet Explorer) 333
Figure 114 Figure 18-4 Security Certificate 1 (Netscape) 334
Figure 115 Security Certificate 2 (Netscape) 335
Figure 116 Logon screen (Internet Explorer) 337
Figure 117 Login screen (Netscape) 338
Figure 118 Replace certificate 339
Figure 119 Device-specific certificate 340
Figure 120 Common Business Secure Router certificate 341
Figure 121 SSH Communication Example 342
Figure 122 How SSH Works 342
Figure 123 SSH 344
Figure 124 SSH Example 1: Store Host Key 345
Figure 125 SSH Example 2: Test 346
Figure 126 SSH Example 2: Log on 347
Figure 127 Secure FTP: Firmware Upload Example 348
Figure 128 Telnet configuration on a TCP/IP network 348
Figure 129 Telnet 349
Figure 130 FTP 350
Figure 131 SNMP Management Model 352
Figure 132 SNMP 354
Figure 133 DNS 356
Figure 134 Security 357

Figure 135 Configuring UPnP 361
Figure 136 UPnP Ports 362
Figure 137 Add/Remove programs: Windows setup 364
Figure 138 Communications 364
Figure 139 Network connections 365
Figure 140 Windows optional networking components wizard 365
Figure 141 Windows XP networking services 366
Figure 142 Internet gateway icon 367
Figure 143 Internet connection properties 367
Figure 144 Internet connection properties advanced setup 368
Figure 145 Service settings 368
Figure 146 Internet connection icon 369
Figure 147 Internet connection status 369
Figure 148 Network connections 370
Figure 149 My Network Places: Local network 370
Figure 150 View Log 372
Figure 151 Log settings 374
Figure 152 Reports 377
Figure 153 Web site hits report example 379
Figure 154 Protocol/Port report example 380
Figure 155 LAN IP address report example 382
Figure 156 Call schedule summary 386
Figure 157 Call schedule edit 387
Figure 158 Applying Schedule Sets to a remote node 390
Figure 159 System Status 392
Figure 160 System Status: Show statistics 393
Figure 161 DHCP Table 395
Figure 162 Firmware upload 396
Figure 163 Firmware Upload In Process 397
Figure 164 Network Temporarily Disconnected 397
Figure 165 Firmware upload error 397
Figure 166 Configuration 398
Figure 167 Reset warning message 399
Figure 168 Configuration Upload Successful 400
Figure 169 Network Temporarily Disconnected 401

Figure 170 Restart screen 402
Figure 171 Pop-up Blocker 408
Figure 172 Internet Options 409
Figure 173 Internet options 410
Figure 174 Pop-up Blocker settings 411
Figure 175 Internet options 412
Figure 176 Security Settings - Java Scripting 413
Figure 177 Security Settings - Java 414
Figure 178 Java (Sun) 415
Figure 179 Allow Popups from this site 416
Figure 180 Netscape Search Toolbar 416
Figure 181 Popup Windows 417
Figure 182 Popup Windows 418
Figure 183 Allowed Sites 419
Figure 184 Advanced 420
Figure 185 Scripts & Plug-ins 421
Figure 186 Example VPN Initiator IPSec Log 433
Figure 187 Example VPN Responder IPSec Log 434

Tables

Table 1 Feature Specifications 33
Table 2 Wizard 2: Ethernet Encapsulation 54
Table 3 Wizard 2: PPTP Encapsulation 55
Table 4 Wizard2: PPPoE Encapsulation 57
Table 5 Private IP Address Ranges 58
Table 6 Example of network properties for LAN servers with fixed IP addresses . 61
Table 7 Wizard 3 62
Table 8 System general setup 79
Table 9 DDNS 82
Table 10 Password 84
Table 11 Default Time Servers 86
Table 12 Time and Date 88
Table 13 ALG 91
Table 14 LAN IP 97
Table 15 Static DHCP 100
Table 16 IP Alias 102
Table 17 WAN: Route 106
Table 18 Ethernet Encapsulation 108
Table 19 PPPoE Encapsulation 110
Table 20 PPTP Encapsulation 111
Table 21 RR Service Type 113
Table 22 WAN: IP 116
Table 23 Traffic Redirect 121
Table 24 Dial Backup Setup 124
Table 25 Advanced Setup 129
Table 26 NAT definitions 132
Table 27 NAT mapping type 136
Table 28 Services and port numbers 138
Table 29 SUA/NAT setup 140

Table 30 Address Mapping 142
Table 31 Address Mapping edit 144
Table 32 Trigger Port 148
Table 33 IP Static Route summary 151
Table 34 Edit IP Static Route 152
Table 35 ICMP commands that trigger alerts 162
Table 36 Legal NetBIOS commands 162
Table 37 Legal SMTP commands 163
Table 38 Firewall rules summary: First screen 178
Table 39 Creating and editing a firewall rule 181
Table 40 Adding or editing source and destination addresses 183
Table 41 Creating/Editing A Custom Port 184
Table 42 Predefined services 189
Table 43 Attack alert 194
Table 44 Content filter 199
Table 45 VPN Screens overview 202
Table 46 VPN Screens Overview 203
Table 47 AH and ESP 207
Table 48 VPN and NAT 210
Table 49 Summary 213
Table 50 VPN Contivity Client rule setup 217
Table 51 VPN Contivity Client advanced rule setup 219
Table 52 Local ID type and content fields 220
Table 54 Matching ID type and content configuration example 221
Table 53 Peer ID type and content fields 221
Table 55 Mismatching ID Type and Content Configuration Example 222
Table 56 VPN Branch Office rule setup 224
Table 57 VPN Branch Office — IP Policy 232
Table 58 VPN Branch Office — IP Policy - Port Forwarding Server 237
Table 59 VPN Branch Office Advanced Rule Setup 242
Table 60 VPN SA Monitor 245
Table 61 VPN Global Setting 247
Table 62 VPN Client Termination 250
Table 63 VPN Client Termination IP pool summary 253
Table 64 VPN Client Termination IP pool edit 254

Table 65 VPN Client Termination advanced 257
Table 66 My Certificates 265
Table 67 My Certificate Import 268
Table 68 My Certificate create 270
Table 69 My Certificate details 274
Table 70 Trusted CAs 277
Table 71 Trusted CA import 279
Table 72 Trusted CA details 282
Table 73 Trusted Remote Hosts 285
Table 74 Trusted remote host import 289
Table 75 Trusted remote host details 291
Table 76 Directory Servers 294
Table 77 Directory server add 295
Table 78 Application and Subnet based Bandwidth Management Example 299
Table 79 Bandwidth Manager: Summary 300
Table 80 Bandwidth Manager: Class Setup 302
Table 81 Bandwidth Manager: Edit class 304
Table 82 Services and port numbers 306
Table 83 Bandwidth management statistics 307
Table 84 Bandwidth manager monitor 308
Table 85 802.1X 312
Table 86 Local User database 316
Table 87 Local User database edit 319
Table 88 Current split networks 321
Table 89 Current split networks edit 322
Table 90 RADIUS 324
Table 91 WWW 331
Table 92 SSH 344
Table 93 Telnet 349
Table 94 FTP 350
Table 95 SNMP traps 353
Table 96 SNMP 354
Table 97 DNS 356
Table 98 Security 357
Table 99 Configuring UPnP 361

Table 100 UPnP Ports 362
Table 101 View Log 372
Table 102 Log settings 375
Table 103 Reports 378
Table 104 Web site hits report 379
Table 105 Protocol/ Port Report 381
Table 106 LAN IP Address Report 382
Table 107 Report Specifications 383
Table 108 Call Schedule Summary 386
Table 109 Call schedule edit 388
Table 110 System Status 392
Table 111 System Status: Show statistics 393
Table 112 DHCP Table 395
Table 113 Firmware Upload 396
Table 114 Restore configuration 400
Table 115 Troubleshooting the Start-Up of your Business Secure Router 403
Table 116 Troubleshooting the LAN LED 404
Table 117 Troubleshooting the LAN Interface 404
Table 118 Troubleshooting the WAN Interface 405
Table 119 Troubleshooting Internet Access 405
Table 120 Troubleshooting Web Site Internet Access 406
Table 121 Troubleshooting the password 406
Table 122 Troubleshooting the WebGUI 407
Table 123 Troubleshooting Remote Management 407
Table 124 System Error Logs 423
Table 125 System Maintenance Logs 423
Table 126 UPnP Logs 424
Table 127 Content Filtering Logs 424
Table 128 Attack Logs 424
Table 129 Access Logs 426
Table 130 ACL Setting Notes 431
Table 131 ICMP Notes 431
Table 132 Sys log 432
Table 133 Sample IKE Key Exchange Logs 435
Table 134 Sample IPSec Logs During Packet Transmission 437

Table 135 RFC-2408 ISAKMP Payload Types 438
Table 136 PKI Logs 438
Table 137 Certificate Path Verification Failure Reason Codes 440
Table 138 IIEEE 802.1X Logs 441
Table 139 Log categories and available settings 442

Preface

Before you begin

This guide assists you through the basic configuration of your Business Secure Router for its various applications.

Note: This guide explains how to use the WebGUI to configure your Business Secure Router. See *Nortel Business Secure Router 222 Configuration — Advanced* (NN47922-501) for how to use the System Management Terminal (SMT) or the command interpreter interface to configure your Business Secure Router. Not all features can be configured through all interfaces.

The WebGUI parts of this guide contain background information on features configurable by the WebGUI and the SMT. For features not configurable by the WebGUI, only background information is provided.

Text conventions

This guide uses the following text conventions:

Enter means type one or more characters and press the enter key. Select or Choose means use one of the predefined choices.

The SMT menu titles and labels are written in **Bold Times New Roman** font.

The choices of a menu choices are written in **Bold Arial** font.

A single keystroke is written in Arial font and enclosed in square brackets. For instance, [ENTER] means the Enter key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

Mouse action sequences are denoted using a comma. For example, “click the **Apple** icon, **Control Panels** and then **Modem**” means first click the **Apple** icon, then point your mouse pointer to **Control Panels** and then click **Modem**.

Related publications

For more information about using the Business Secure Router, refer to the following publications:

- *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301)

  This guide helps you get up and running right away. It contains connection information and instructions on getting started.

- *Nortel Business Secure Router 222 Configuration — Advanced* (NN47922-501)

  This guide covers how to use the SMT menu to configure your Business Secure Router.

- *WebGUI Online Help*

  Embedded WebGUI help is available to provide descriptions of individual screens and supplementary information.

Hard copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/documentation. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of Adobe Reader.

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 1
Getting to know your Nortel Business Secure Router 222

This chapter introduces the main features and applications of the Business Secure Router.

Introducing the Nortel Business Secure Router 222

The Nortel Business Secure Router 222 is an ideal secure gateway for all data passing between the Internet and the Local Area Network (LAN).

By integrating Network Address Translation (NAT), firewall and Virtual Private Network (VPN) capability, the Business Secure Router is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The embedded WebGUI assists in easy setup and management of the Business Secure Router via an Internet browser.

Features

This section lists the key features of the Business Secure Router.

Table 1 Feature Specifications

Feature	Specification
Number of static routes	12
Number of NAT sessions	4096
Number of SUA servers	12

Table 1 Feature Specifications

Feature	Specification
Number of address mapping rules	10
Maximum number of VPN IP Policies	60
Maximum number of VPN Tunnels (Client and/or Branch Office)	10
Maximum number of concurrent VPN IPSec Connections	60
Number of IP pools can be used to assign IP addresses to remote users for VPN client termination	3
Number of configurable split networks for VPN client termination	16
Number of configurable inverse split networks for VPN client termination	16
Number of configurable subnets per split network for VPN client termination	64

Physical features

4-Port switch

A combination of switch and router makes your Nortel Business Secure Router 222 a cost effective and viable network solution. You can connect up to four computers or phones to the Business Secure Router without the cost of a switch. Use a switch to add more than four computers or phones to your LAN.

Autonegotiating 10/100 Mb/s Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mb/s Ethernet.

Autosensing 10/100 Mb/s Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight through Ethernet cable.

Autonegotiating 10/100 Mb/s Ethernet WAN

The 10/100 Mb/s Ethernet WAN port attaches to the Internet via broadband modem or router and automatically detects if it is on a 10 or a 100 Mb/s Ethernet.

Auxiliary port

The Business Secure Router uses the same port for console management and for an auxiliary WAN backup. The AUX port can be used in reserve as a traditional dial-up connection when or if ever the broadband connection to the WAN port fails.

Time and date

Using the Business Secure Router, you can get the current time and date from an external server when you turn on your Business Secure Router. You can also set the time manually.

Reset button

The Business Secure Router reset button is built into the rear panel. Use this button to restart the Business Secure Router or restore the factory default password to PlsChgMe!, IP address to 192.168.1.1, subnet mask to 255.255.255.0, and DHCP server enabled with a pool of 126 IP addresses starting at 192.168.1.2.

Nonphysical features

IPSec VPN capability

Establish Virtual Private Network (VPN) tunnels to connect home or office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Nortel Contivity Client Termination

The Business Secure Router supports VPN connections from computers using Nortel Contivity VPN Client 3.0, 5.01, 5.11, 6.01, 6.02, or 7.01 software.

Certificates

The Business Secure Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

SSH

The Business Secure Router uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure WebGUI access to the Business Secure Router.

IEEE 802.1x for network security

The Business Secure Router supports the IEEE 802.1x standard for user authentication. With the local user profile in the Business Secure Router, you can configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server.

Firewall

The Business Secure Router has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Business Secure Router firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

Brute force password guessing protection

The Business Secure Router has a special protection mechanism to discourage brute force password guessing attacks on the Business Secure Router's management interfaces. You can specify a wait time that must expire before you can enter a fourth password after entering three incorrect passwords.

Content filtering

The Business Secure Router can block web features such as ActiveX controls, Java applets, and cookies, as well as disable web proxies. The Business Secure Router can block specific URLs by using the keyword feature. The administrator can also define time periods and days during which content filtering is enabled.

Packet filtering

The packet filtering mechanism blocks unwanted traffic from entering or leaving your network.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Business Secure Router and other UPnP-enabled devices can dynamically join a network, obtain an IP address, and convey its capabilities to other devices on the network.

Call scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar dial-up networking user interface.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network.

PPTP supports on-demand, multiprotocol, and virtual private networking over public networks, such as the Internet. The Business Secure Router supports one PPTP server connection at any given time.

Dynamic DNS support

With Dynamic DNS (Domain Name System) support, you can have a static host name alias for a dynamic IP address, so the host is more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

IP Multicast

The Business Secure Router can use IP multicast to deliver IP packets to a specific group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The Business Secure Router supports versions 1 and 2.

IP Alias

Using IP Alias, you can partition a physical network into logical networks over the same Ethernet interface. The Business Secure Router supports three logical LAN interfaces via its single physical Ethernet LAN interface with the Business Secure Router itself as the gateway for each LAN network.

Central Network Management

With Central Network Management (CNM), an enterprise or service provider network administrator can manage your Business Secure Router. The enterprise or service provider network administrator can configure your Business Secure Router, perform firmware upgrades, and do troubleshooting for you.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Business Secure Router supports SNMP agent functionality, which means that a manager station can manage and monitor the Business Secure Router through the network. The Business Secure Router supports SNMP versions 1 and 2 (SNMPv1 and SNMPv2).

Network Address Translation (NAT)

NAT (Network Address Translation — NAT, RFC 1631) translate multiple IP addresses used within one network to different IP addresses known within another network.

Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway when the Business Secure Router cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You can enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

With DHCP (Dynamic Host Configuration Protocol), individual client computers can obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Business Secure Router has built in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway, and DNS servers to all systems that support the DHCP client. The Business Secure Router can also act as a surrogate DHCP server, where it relays IP address assignment from another DHCP server to the clients.

Full network management

The embedded web configurator is an all platform, web based utility that you can use to easily manage and configure the Business Secure Router. Most functions of the Business Secure Router are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu driven interface that you can access from a terminal emulator through the console port or over a Telnet connection.

Road Runner support

In addition to standard cable modem services, the Business Secure Router supports Time Warner's Road Runner Service.

Logging and tracing

The Business Secure Router supports the following logging and tracing functions to help with management:

- Built in message logging and packet tracing
- Unix syslog facility support

Upgrade Business Secure Router Firmware

The firmware of the Business Secure Router can be upgraded via the console port or the LAN.

Embedded FTP and TFTP Servers

The Business Secure Router's embedded FTP and TFTP Servers enable fast firmware upgrades, as well as configuration file backups and restoration.

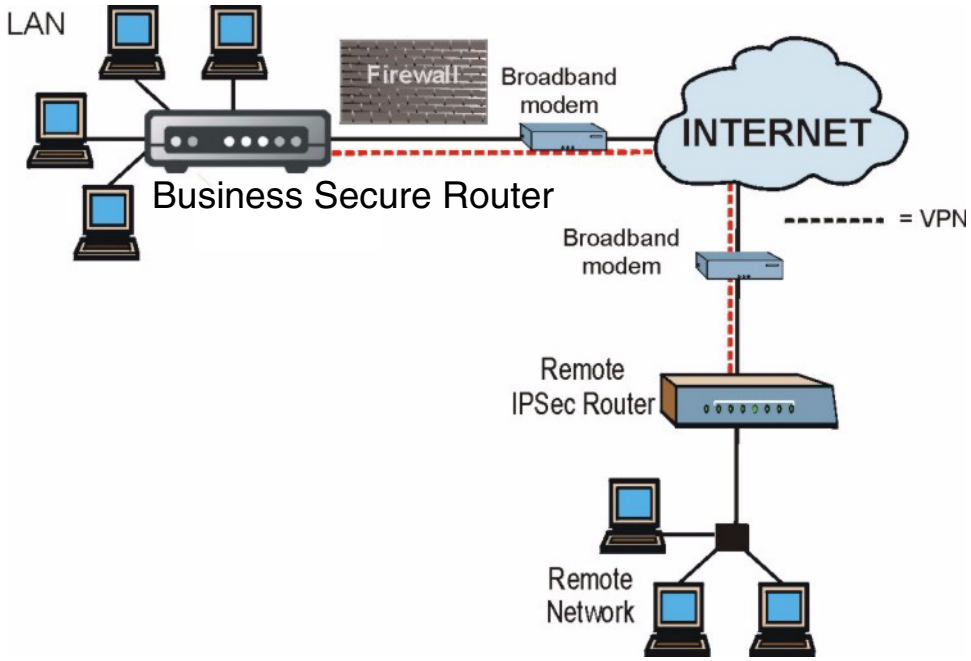
Applications for the Nortel Business Secure Router 222

Secure broadband internet access and VPN

You can connect a cable, DSL, or other modem to the Nortel Business Secure Router 222 via Ethernet WAN port for broadband Internet access. The Business Secure Router also provides IP address sharing and a firewall protected local network with traffic management.

VPN is an ideal, cost effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can share the VPN tunnels for secure connections to remote computers.

Figure 1 Secure Internet Access and VPN Application



Hardware Setup

Refer to *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301) for hardware connection instructions.

Note: To keep the Business Secure Router operating at optimal internal temperature, keep the bottom, sides, and rear clear of obstructions and away from the exhaust of other equipment.

After installing your Nortel Business Secure Router 222, continue with the rest of this guide for configuration instructions.

Chapter 2
Introducing the WebGUI

This chapter describes how to access the Business Secure Router WebGUI and provides an overview of its screens.

WebGUI overview

The WebGUI is an HTML based management interface that a user can use for easy setup and management of the Business Secure Router via an Internet browser.

Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1 024 by 768 pixels.

In order to use the WebGUI you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See "Allowing Pop-up Windows, JavaScript and Java Permissions" on page 408 if you want to make sure these functions are allowed in Internet Explorer.

Accessing the Business Secure Router WebGUI

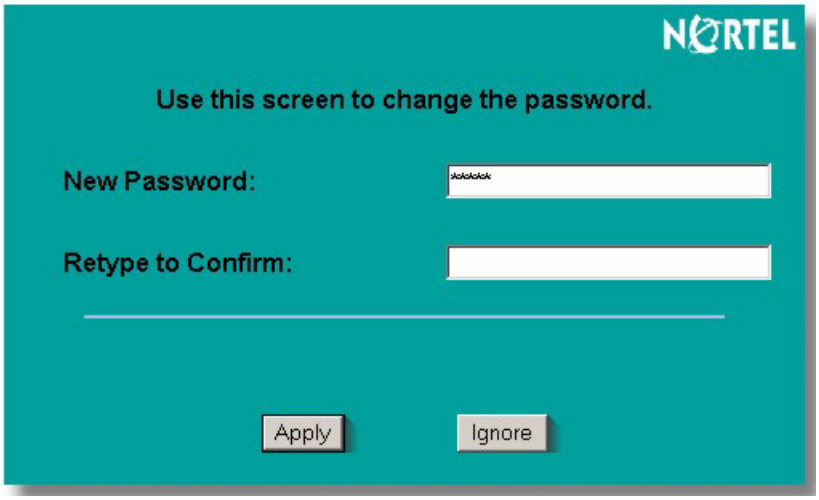
Make sure your Business Secure Router hardware is properly connected and prepare your computer and computer network to connect to the Business Secure Router. Refer to the *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301).

1. Launch your web browser.
2. Type 192.168.1.1 as the URL.
3. Type the user name (nnadmin is the default) and the password (PlsChgMe! is the default) and click **Login**. Click **Reset** to clear any information you have entered in the **Username** and **Password** fields.

Figure 2 Login screen

4. A screen asking you to change your password (highly recommended) appears and is shown in Figure 3. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 3 Change password screen



5 Click **Apply** in the **Replace Certificate** screen to create a certificate using your Business Secure Router's MAC address that is specific to this device.

Figure 4 Replace certificate screen

NORTEL
Replace Factory Default Certificate
The factory default certificate is common to Business Secure Router series models. Click Apply to create a certificate using your Business Secure Router 's MAC address that will be specific to this device.
Apply
Ignore

The **MAIN MENU** screen appears.

Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back on to the Business Secure Router if this happens to you.

Restoring the factory default configuration settings

If you just want to restart the Business Secure Router, press the rear panel **RESET** button for one to three seconds.

If you forget your password or cannot access the SMT menu, you must reload the factory default configuration file or use the **RESET** button the back of the Business Secure Router to restore the factory default configuration. Uploading this configuration file replaces the current configuration file with the factory default configuration file. All previous configurations are lost, and the speed of the console port is reset to the default of 9 600 bp/s with 8 data bit, no parity, one stop bit and flow control set to none. The password is also reset to PlsChgMe!.

Procedure to use the reset button

Press the rear panel **RESET** button for longer than three seconds to return the Business Secure Router to the factory defaults.

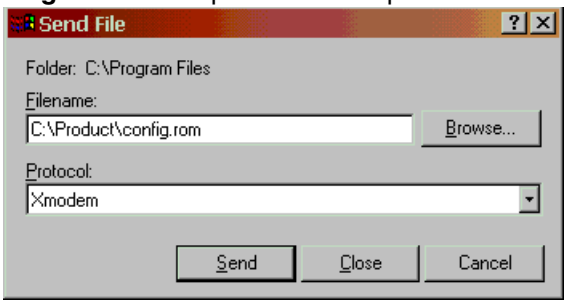
Uploading a configuration file via console port

1. Download the default configuration file from the Nortel FTP site, unzip it and save it in a folder.
2. Turn off the Business Secure Router, begin a terminal emulation software session and turn on the Business Secure Router again. When you see the message Press Any key to enter Debug Mode within 3 seconds, press any key to enter debug mode.
3. Enter y at the prompt to go into debug mode.
4. Enter atlc after the Enter Debug Mode message displays.

5 Wait for the Starting XMODEM upload message before activating Xmodem upload on your terminal. Figure 5 is an example of an Xmodem configuration upload using HyperTerminal.

6 Click **Transfer**, then **Send File** to display the screen illustrated in Figure 5.

Figure 5 Example Xmodem Upload



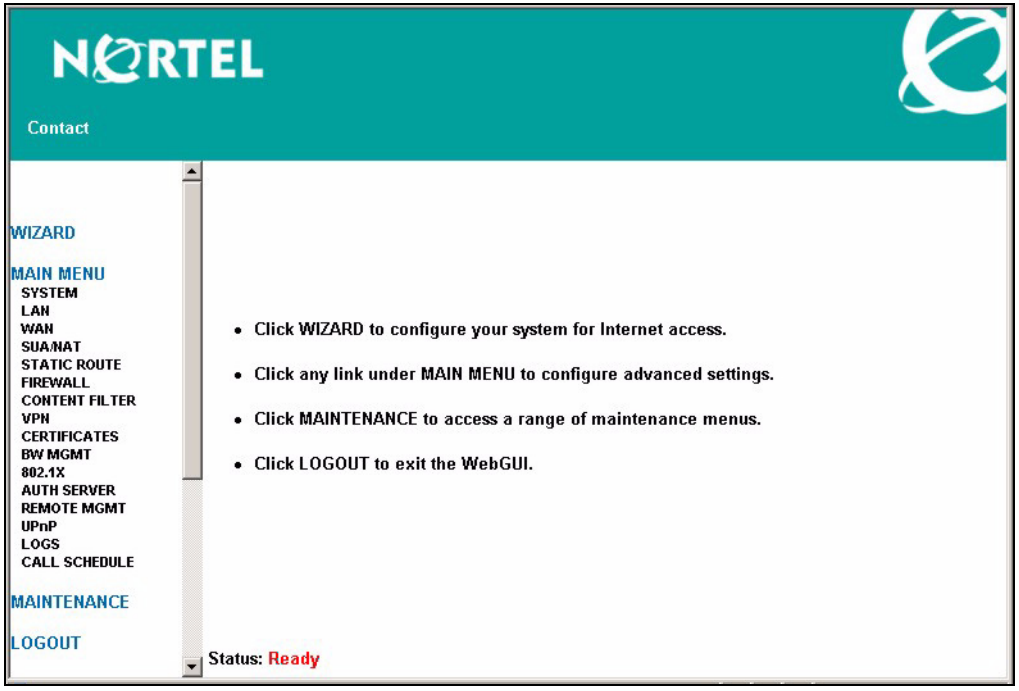
7 After the firmware uploads successfully, enter atgo to restart the router.

Navigating the Business Secure Router WebGUI

Follow the instructions in the MAIN MENU screen or click the help icon (located in the top right corner of most screens) to view online help.

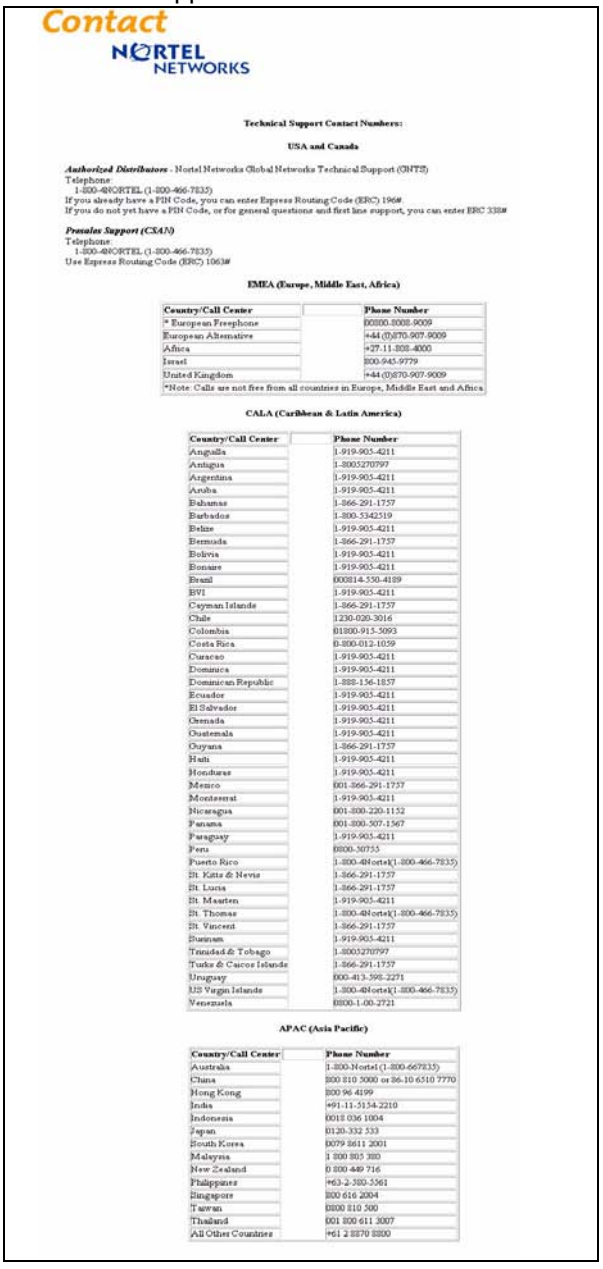
Note: The help icon does not appear in the MAIN MENU screen.

Figure 6 MAIN MENU Screen



Click the **Contact** link to display the customer support contact information. Figure 7 is a sample of what displays.

Figure 7 Contact Support



Contact

NORTEL NETWORKS

Technical Support Contact Numbers:

USA and Canada

Authorized Distributors - Nortel Networks Global Networks Technical Support (GNTS)
Telephone:
1-800-4NORTEL (1-800-466-7835)
If you already have a PIN Code, you can enter Express Routing Code (ERC) 196#.
If you do not yet have a PIN Code, or for general questions and first line support, you can enter ERC 338#

Presales Support (CSAN)
Telephone:
1-800-4NORTEL (1-800-466-7835)
Use Express Routing Code (ERC) 1063#

EMEA (Europe, Middle East, Africa)

Country/Call Center		Phone Number
* European Freephone		00800-8008-9009
European Alternative		+44 (0)870-907-9009
Africa		+27-11-808-4000
Israel		800-945-9779
United Kingdom		+44 (0)870-907-9009

*Note: Calls are not free from all countries in Europe, Middle East and Africa.

CALA (Caribbean & Latin America)

Country/Call Center		Phone Number
Anguilla		1-919-905-4211
Antigua		1-8005270797
Argentina		1-919-905-4211
Aruba		1-919-905-4211
Bahamas		1-866-291-1757
Barbados		1-800-5342519
Belize		1-919-905-4211
Bermuda		1-866-291-1757
Bolivia		1-919-905-4211
Bonaire		1-919-905-4211
Brasil		000814-550-4189
BVI		1-919-905-4211
Cayman Islands		1-866-291-1757
Chile		1230-020-3016
Colombia		01800-915-5093
Costa Rica		0-800-012-1059
Curacao		1-919-905-4211
Dominica		1-919-905-4211
Dominican Republic		1-888-156-1857
Ecuador		1-919-905-4211
El Salvador		1-919-905-4211
Grenada		1-919-905-4211
Guatemala		1-919-905-4211
Guyana		1-866-291-1757
Haiti		1-919-905-4211
Honduras		1-919-905-4211
Mexico		001-866-291-1757
Montserrat		1-919-905-4211
Nicaragua		001-800-220-1152
Panama		001-800-507-1567
Paraguay		1-919-905-4211
Peru		0800-50755
Puerto Rico		1-800-4Nortel(1-800-466-7835)
St. Kitts & Nevis		1-866-291-1757
St. Lucia		1-866-291-1757
St. Maarten		1-919-905-4211
St. Thomas		1-800-4Nortel(1-800-466-7835)
St. Vincent		1-866-291-1757
Surinam		1-919-905-4211
Trinidad & Tobago		1-8005270797
Turks & Caicos Islands		1-866-291-1757
Uruguay		000-413-598-2271
US Virgin Islands		1-800-4Nortel(1-800-466-7835)
Venezuela		0800-1-00-2721

APAC (Asia Pacific)

Country/Call Center		Phone Number
Australia		1-800-Nortel (1-800-667835)
China		800 810 5000 or 86-10 6510 7770
Hong Kong		800 96 4199
India		+91-11-5154-2210
Indonesia		0018 036 1004
Japan		0120-332 533
South Korea		0079 8611 2001
Malaysia		1 800 805 380
New Zealand		0 800 449 716
Philippines		+63-2-380-5561
Singapore		800 616 2004
Taiwan		0800 810 500
Thailand		001 800 611 3007
All Other Countries		+61 2 8870 8800

Chapter 3
Wizard setup

This chapter provides information on the Wizard screens in the WebGUI.

Wizard overview

The setup wizard in the WebGUI helps you configure your device to access the Internet. The second screen has three variations, depending on which encapsulation type you use. Refer to your ISP checklist in the *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301) to know what to enter in each field. Leave a field blank if you do not have the required information.

Wizard setup: General Setup and System Name

General Setup contains administrative and system related information. **System Name** is for identification purposes. However, because some ISPs check this name, you must enter your Computer Name.

In Windows 95/98, click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.

In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.

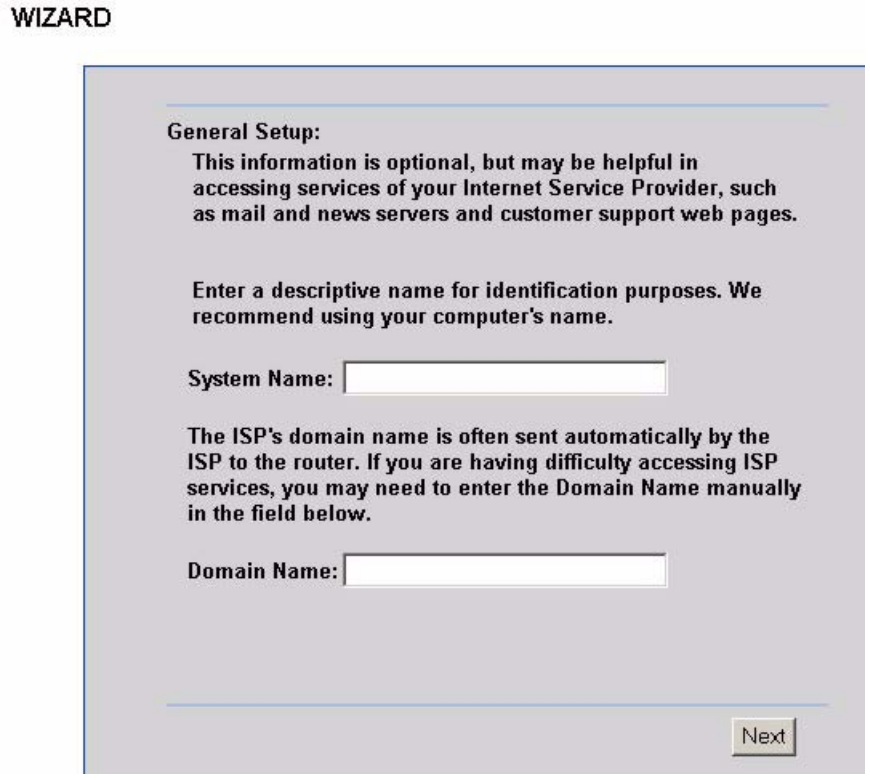
In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Business Secure Router **System Name**.

Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Business Secure Router via DHCP.

Click **Next** to configure the Business Secure Router for Internet access.

Figure 8 Wizard 1


WIZARD
General Setup:
This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.
Enter a descriptive name for identification purposes. We recommend using your computer's name.
System Name:
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
Domain Name:
Next

Wizard setup: Screen 2

The Business Secure Router offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE.**

Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 9 Wizard 2: Ethernet Encapsulation

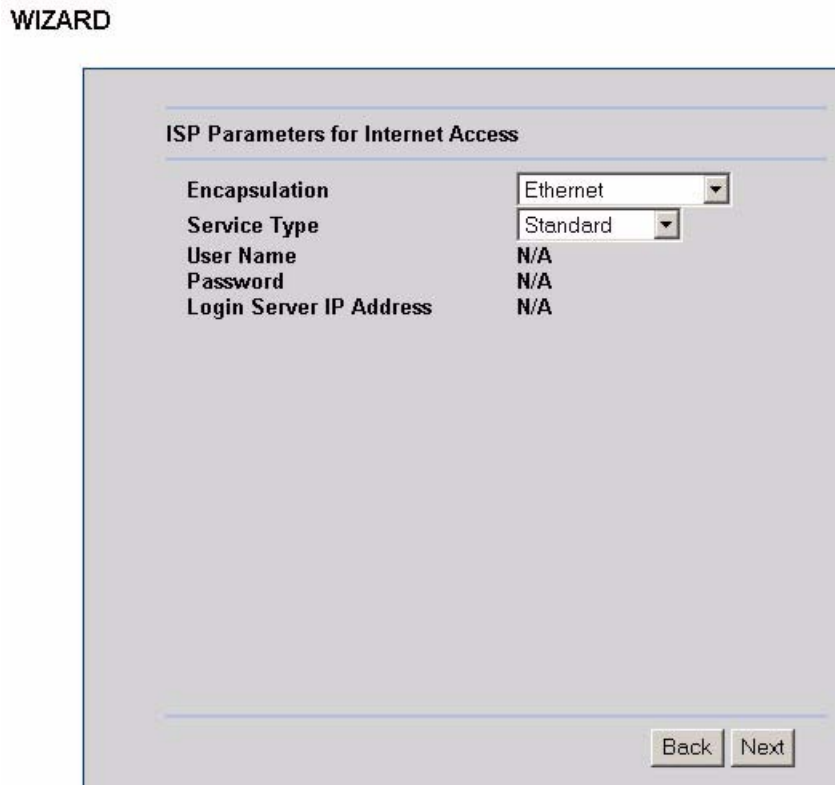


Table 2 describes the fields in Figure 9.

Table 2 Wizard 2: Ethernet Encapsulation

Label	Description
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
Service Type	Choose from **Standard**, **RR-Telstra** (Telstra authentication method), **RR-Manager** (Road Runner Manager authentication method) or **RR-Toshiba** (Road Runner Toshiba authentication method). For ISPs (such as Telstra) that send UDP-heartbeat packets to verify that the customer is still online, create a WAN-to-WAN/ Business Secure Router firewall rule that allows access for port 1026 (UDP). The following fields are not applicable (**N/A**) for the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multiprotocol, and virtual private networking over public networks, such as the Internet.

Note: The Business Secure Router supports one PPTP server connection at any given time

Figure 10 Wizard 2: PPTP Encapsulation

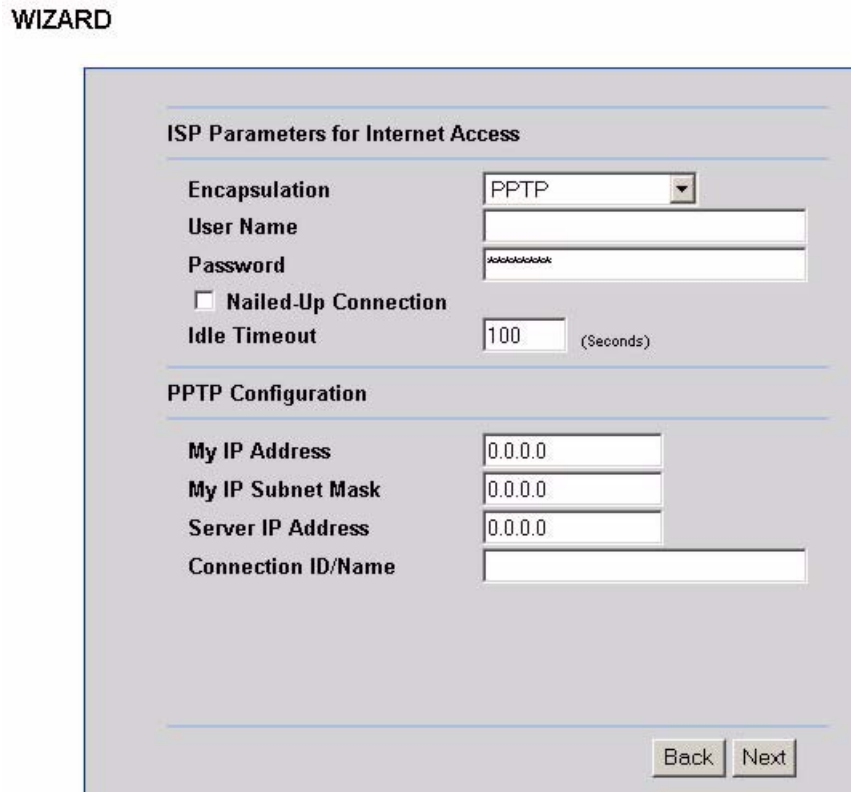


Table 3 describes the fields in Figure 10.

Table 3 Wizard 2: PPTP Encapsulation

Label	Description
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list.
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the username above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time, in seconds, that elapses before the router automatically disconnects from the PPTP server. The default is 45 seconds.

Table 3 Wizard 2: PPTP Encapsulation

Label	Description
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the c:id and n:name format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example, DSL, cable, or wireless) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a logon and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This means the service provider can easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP or carrier, as it requires no specific configuration of the broadband modem at the subscriber site.

By implementing PPPoE directly on the Business Secure Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Business Secure Router does that part of the task. Furthermore, with NAT, all the computers on the LAN have Internet access.

Figure 11 Wizard2: PPPoE Encapsulation

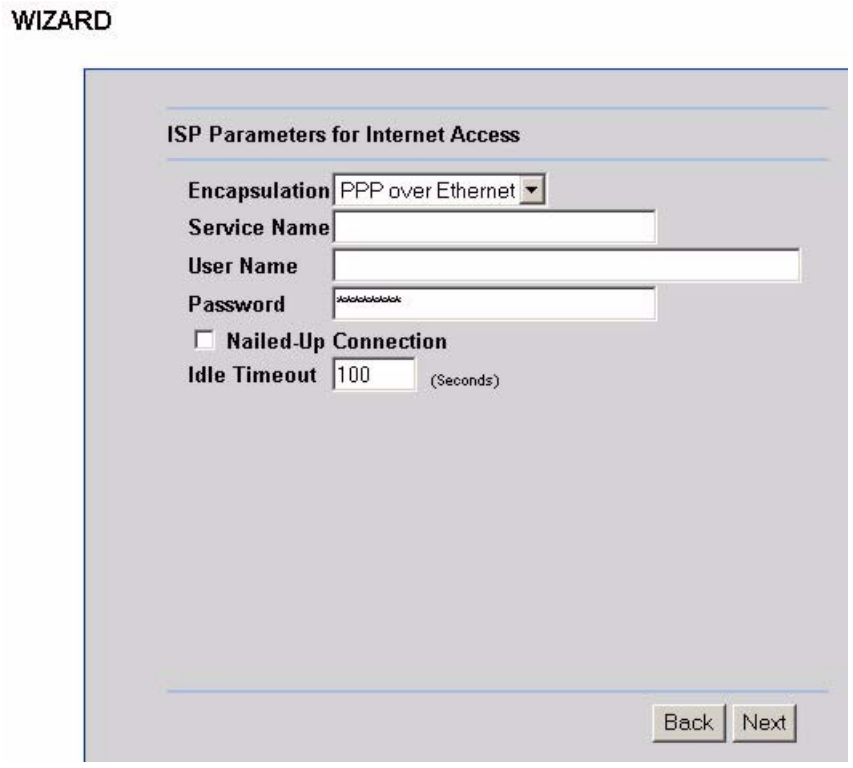


Table 4 describes the fields in Figure 11.

Table 4 Wizard2: PPPoE Encapsulation

Label	Description
Encapsulation	Select **PPP over Ethernet** from the drop-down list.
Service Name	Type the name of your service provider.
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the username above.

Table 4 Wizard2: PPPoE Encapsulation

Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time, in seconds, that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

Wizard setup: Screen 3

Using the third screen you can configure WAN IP address assignment, DNS server address assignment, and the WAN MAC address.

WAN IP address assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, it only connects your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved three blocks of IP addresses specifically for private networks.

Table 5 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. If you are part of a much larger organization, consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information about address assignment, refer to *Address Allocation for Private Internets* (RFC 1597), and *Guidelines for Management of IP Address Space* (RFC 1466).

IP address and Subnet Mask

Similar to the way houses on a street share a common street name, computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If your ISP or network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If your ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, Nortel recommends that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Business Secure Router. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; do not use any other number unless you are told otherwise. For example, select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number, while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Business Secure Router, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Business Secure Router computes the subnet mask automatically based on the IP address that you enter. You do not need to change the subnet mask computed by the Business Secure Router unless you are instructed to do otherwise.

DNS Server address assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.nortel.com is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Business Secure Router can get the DNS server addresses in the following ways:

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
- If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

WAN MAC address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the MAC address of the WAN port by either using the factory default or cloning the MAC address from a computer on your LAN. Once the MAC address of the WAN port is successfully configured, the address is copied to the rom file (configuration file) and does not change unless you change the setting or upload a different rom file.

The WAN port of your Business Secure Router is set at half-duplex mode, as most cable or DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your Business Secure Router supports full duplex mode on the LAN side.

Table 6 Example of network properties for LAN servers with fixed IP addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Business Secure Router LAN IP)

The third wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

Figure 12 Wizard 3

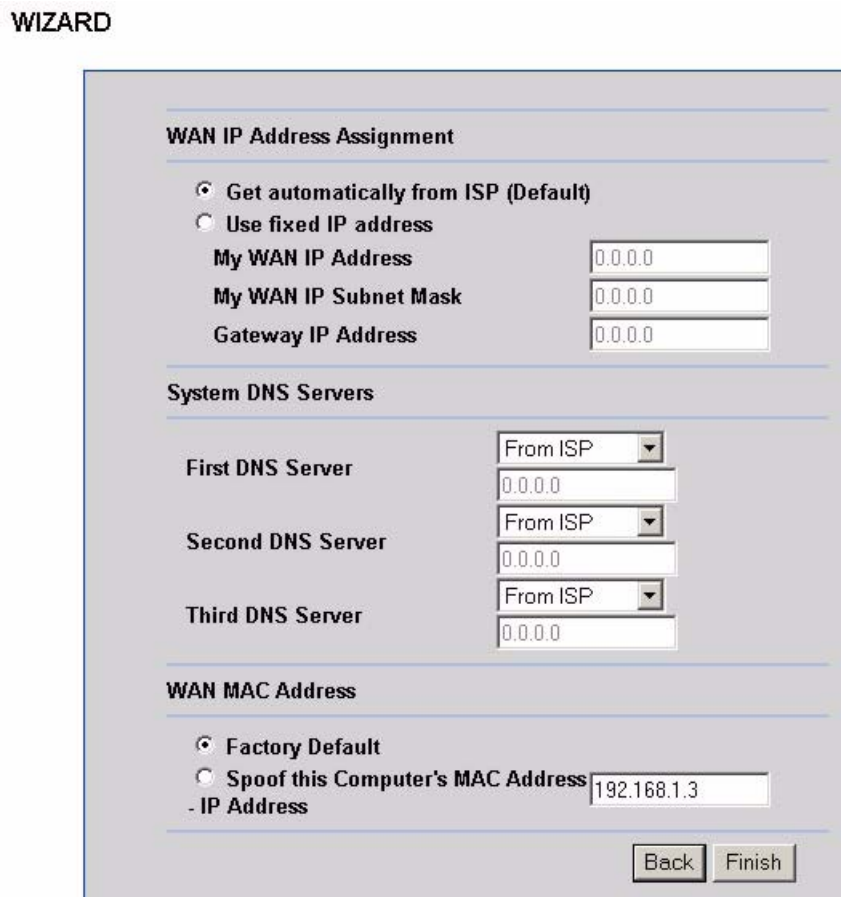


Table 7 describes the fields in Figure 12.

Table 7 Wizard 3

Label	Description
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you select **Use Fixed IP Address.**

Table 7 Wizard 3

Label	Description
IP Subnet Mask	Enter the IP subnet mask in this field if you select **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
Gateway IP Address	Enter the gateway IP address in this field if you select **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
DNS Server Address Assignment	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. For example, the IP address of www.nortel.com is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
	System DNS Servers (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Business Secure Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Table 7 Wizard 3

Label	Description
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Business Secure Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Business Secure Router has a fixed WAN IP address, **From ISP** changes to **None** after you click **Finish**. If you chose **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after you click **Finish**. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. Select **Private DNS** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in the **LAN IP** screen to use **DNS Relay**. You must also configure a VPN branch office rule since the Business Secure Router uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the Business Secure Router as a local IP address and the IP address of the DNS server as a remote IP address. A **Private DNS** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **Private DNS** entry changes to **None** after you click **Apply**.
WAN MAC Address	In the MAC Address field, you can configure the MAC address of the WAN port by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. After it is successfully configured, the address is copied to the rom file (configuration file). It does not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

Basic Setup Complete

Well done! You have successfully set up your Business Secure Router to operate on your network and access the Internet.

Chapter 4
User Notes

General Notes

There are some router functions that, although performing as expected, might cause some confusion. These are summarized below.

General

1 Default Address Mapping Rules When First Enable NAT Full Feature.

When NAT Full Feature is first enabled, two address mapping rules are added to the address mapping table. This is done to facilitate programming, and matches the default SUA rule. The rules can be deleted.

2 Response to Invalid User ID or Password

When the wrong user ID or password is entered into the router login screen, no error message is displayed. Instead, the login screen is simply displayed again.

3 First DHCP Address Reserved for BCM50

The first address of the DHCP Address Pool is reserved for a BCM50 in the subnet, and will not be assigned to any other equipment. Once assigned to a BCM50, it is reserved for that BCM50, and will not be assigned to any other. If the BCM50 is changed, the following command must be used to enable the router to assign the first address to a different BCM50:

```
ip dhcp enif0 server m50mac clear
```

4 Login Requires Reboot

If the Administrator Timeout is set to 0, and an administration session is terminated without logging off, the router needs to be rebooted in order for the administrator to log in to the WebGUI again. Alternatively, the administrator can log in using a TelNet session, if TelNet access has been enabled in the Remote Management menu.

5 Clicking Sound

The Business Secure Router will click once every two minutes until an ADSL line is connected.

Firewall

1 Address Range Validation

In the firewall rules, the router does not confirm when given an address range, that the second address is higher than the first. If this type of address range is entered, the range is ignored.

2 Automatic Firewall Programming

Configurations to various areas of the router, such as remote management or adding a SUA Server, do not automatically add the appropriate rules to the Firewall, to enable the traffic to pass through the router. These need to be added separately.

Note: Firewall rules do not apply to IPSec tunnels.

NAT

1 Deleting NAT Rule Does Not Drop an Existing Connection

If a NAT rule is deleted, the router must be rebooted to apply the change to existing service connections. This is already noted in the GUI.

2 NAT Traversal Status

If NAT Traversal is enabled, but is not needed (because the client is not behind a NAT router), it will be shown as 'inactive' in the VPN Client Monitor. This may confuse some users.

VPN Client Termination

1 Change of User Account Does Not Drop Existing Connections

If a VPN Client user account is de-activated, deleted, or changed, and that user is currently connected, the connection is not automatically dropped. To drop the connection, the administrator needs to disconnect the user using the 'Disconnect' function in the VPN/SA Monitor GUI. This is consistent with other Nortel Contivity products.

2 User Name Restrictions

User names are limited to a maximum length of 63 characters.

3 VPN Client Account Password Restrictions

The password for a VPN Client user cannot contain the single- or double-quote characters.

4 IP Pool Address Overlap

When defining multiple VPN Client Termination IP pools, the router uses the IP Subnet mask, and not the pool size, to determine if the pools are overlapping. The subnet mask of each pool should be appropriate for the size of the VPN Client Termination IP pool.

5 VPN Client Termination - Failure In Specific Addressing Situation

If the Client has an assigned IP address that is the same as the IP address assigned for the Client Tunnel, the connection will fail to be established.

6 VPN Client Termination - Configuration Restrictions

This router has some restrictions when compared to larger Contivity Routers (1000 Series and above). In particular,

VPN Clients cannot be added to the LAN subnet. They must have addresses outside of the LAN subnet.

VPN Clients can have dynamically assigned IP addresses, or they can have a statically assigned addresses. However, the router does not support both modes at once. All addresses must either be dynamically assigned, or they must all be statically assigned.

7 Establishing a Client Tunnel From One Business Secure Router to Another

When defining a Client Termination account for another Business Secure Router that will connect using Contivity Client Emulation, the following configuration is required:

- Encryption must be Triple DES with SHA1 integrity, or Triple DES with MD5 integrity.
- IKE Encryption must be Triple DES with Diffie-Hellman Group 2.
- Perfect Forward Secrecy (PFS) must be enabled.

Security

1 Exporting or Saving Self-Signed Certificate

To export or save a self-signed certificate, click details (the icon that looks like a paper note), then click 'Export' or copy the PEM text into the clipboard, and paste into a file.

Routing

1 RIP Version Advertisement Control

To change the version of generated RIP advertisements, the following CLI command needs to be used

ip rip mode [enif0|enif1] [in|out] [0|1|2|3]

where:

'enif0' is the LAN side, and 'enif1' is the WAN side

'in' affects recognition of received advertisements, and

'out' applies to generated advertisements

The number controls the operating mode:

None (disabled)

RIP-1 only

RIP-2 only

Both RIP-1 and RIP-2

Advanced Router Configuration

The following notes are intended to help with advanced router configuration.

Setting up the router when the system has a server

1. If you are using a Full-Feature NAT configuration, first, do the following...
   a. In SUA/NAT / Address Mapping, add a 'Server' rule, specifying the 'Public' IP address of the server.
2. For both SUA-Only and Full-Feature NAT configurations, do the following...
   a. In SUA/NAT : SUA Server, add server private IP address and port number(s) to the SUA/NAT Server table.
   b. In FIREWALL, add a WAN-to-LAN rule
   c. If the service is not in the list of available services, add it as a 'Custom Port'.
   d. Add the rule, selecting the service, and entering the server IP address as the destination IP address.

Connecting two sites to establish a virtual private network

The recommended method to do this is through a branch-to-branch IPSec tunnel.

1. In VPN / Summary, add a new tunnel by editing an unused rule. Create an Active, Branch Office tunnel.
   a. Select 'Nailed Up' if the tunnel should not be closed while not in use.

b Enter the authentication information, with either a pre-shared key or an imported certificate.

c Enter the IP Address assigned to the router WAN port. This should be a static address, or a dynamic DNS name, and the IP address of the remote router.

d Select the encryption and authentication algorithms.

e Add an IP policy, by specifying the IP address ranges of the local and remote hosts that will use the tunnel.

2 Repeat these steps at the other end of the branch.

Note: If VPN Client Termination is used on these sites, the client termination address range will need to be included in the tunnel policies in order for the VPN clients to see the other site.

Adding IP telephony to a multi-site network

Scenario 1: A BCM50 in the primary site acting as the gateway for both sites

1 Ensure that the DHCP Server in the BCM50 is disabled, that the BCM50 is connected to the router, and both have booted.

2 Add the IP phones to the primary site as per BCM50 installation guide.

3 Create a tunnel to the remote site, as described above.

4 In the remote site, set the S1 and S2 addresses to the IP address of the BCM50, which is identified in the router DHCP table or in the BCM50. This is done with a CLI command.

TELNET or SSH to the router. This needs TELNET or SSH enabled on that router. Select menu 24, select menu 8, and enter the commands:

ip dhcp enif0 server voipserver 1 <BCM50_IP_Address> 7000 1

ip dhcp enif0 server voipserver 2 <BCM50_IP_Address> 7000 1

5 Add the IP phones to the remote site, configured for full DHCP client mode.

Scenario 2: A BCM50 in each site, each acting as the backup call server for the other site

1 At each site,

   a Ensure that the DHCP Server in the BCM50 is disabled, that the BCM50 is connected to the router, and both have booted.

   b Add the IP phones to the site as per BCM50 installation guide.

   c At each router, change the S2 address to the IP address of the remote BCM50, using TELNET or SSH, and the CLI command,

   ip dhcp enif0 server voipserver 2 <Remote_BCM50_IP_Address> 7000 1

2 Create a tunnel between the sites, as described above.

3 Create an H.323 trunk between the BCM50s, as per the BCM50 User Guide.

Configuring the router to act as a Nortel VPN Server (Client Termination)

1 Under VPN / Client Termination,

   a Enable Client Termination.

   b Select authentication type and the encryption algorithms supported.

   c If the clients are assigned IP addresses from a pool, define the pool, and enable it.

2 Assuming a Local User Database is used for authentication,

   a Add user name and password to the local user database as an IPSec user, and activate it. If the hosts will be assigned a static IP address, enter the address that will be assigned to the user.

Configuring the router to connect to a Nortel VPN Server (Client Emulation)

1 Go to VPN / Summary, and select 'Edit'.

2 Select a connection type of Contivity Client, and fill in the web page with the relevant data.

3 If Group authentication or On-Demand Client Tunnels are needed, click the 'Advanced' button to configure this.

Allowing remote management of a LAN-connected BCM50

1 Create the appropriate NAT server rules to add the BCM50.

Go to SUA/NAT / SUA Server, and create two server rules for HTTPS and Element Manager access:

One named BCM_HTTPS, with port number 443, and the IP address of the BCM50

One named BCM_EM, with the port number 5989, and the IP address of the BCM50

Note: In DHCP Server mode, the BCM50 IP address will be the lowest address in the pool.

2 Create the appropriate Firewall rules to add BCM50 access.

Go to FIREWALL / Summary, and create two WAN-to-LAN firewall rules:

One rule allowing access from allowed remote computer IP addresses, to the BCM50 IP address, for service type HTTPS(TCP:443)

One rule allowing access from allowed remote computer IP addresses, to the BCM50 IP address, for custom port TCP:5989

Setting up the router for guest access

The recommended approach to provide guest access is by creating an IP Alias, and using static addressing for the corporate equipment, to make it a member of the defined Alias subnet. Then use firewall rules to restrict access of the guest equipment. NOTE: if a BCM50 is used, it will also need to be assigned a static IP address.

1 Go to LAN / IP Alias, and Enable IP Alias 1.

2 Define a subnet for the corporate equipment.

3 Statically assign addresses to the corporate equipment that are within the IP Alias subnet.

4 Set up LAN / IP to enable DHCP Server, with an address range that will be used for guest equipment.

5 In the FIREWALL, set up a LAN-to-LAN rule to block traffic between the guest subnet (DHCP Pool) and the corporate subnet (IP Alias subnet).

Note: If branch tunnels are being used, the policies on these tunnels should exclude the guest subnet.

Preventing heavy data traffic from impacting telephone calls

To ensure voice quality during heavy data traffic, bandwidth needs to be reserved for voice traffic.

1 Determine your actual WAN up-stream bandwidth by connecting to a web site such as http://myvoipspeed.visualware.com/.

2 On BANDWIDTH MANAGEMENT / Summary, activate WAN bandwidth management, and fill in your actual uplink speed in the WAN Speed field..

3 On BANDWIDTH MANAGEMENT / Class Setup, add a WAN subclass, and reserve sufficient bandwidth based on the number of telephones, for Protocol ID 17 (UDP Traffic).

The amount of bandwidth should be based on a reasonable peak number of simultaneous calls, and the data rate needed by the IP telephony CODECs.

Setting Up a Remote Office with a UNIStim IP Telephone

For a remote office with a PC, and a UNIStim IP telephone behind a Business Secure Router, Client Emulation is the recommended method to connect to the main office.

1 At the main office Contivity Client Server, establish two user accounts - one for the telephone, and one for the PC.

2 On the remote office Business Secure Router, do the following:

Under WAN / WAN IP, ensure that Network Address Translation is set to SUA Only (default). Also ensure that the Gateway IP address is set (not 0.0.0.0).

Under VPN / Summary, create an entry for the IP telephone client tunnel. (Contivity Client, Active, Keep Alive). Fill in the IP address of the Contivity Client Server, and the name and password of the telephone set user account.

Under VPN / Global Setting, enable Exclusive Mode, and fill in the MAC address of the telephone set.

Under Bandwidth Management, set up WAN bandwidth management to reserve 110 kbps of bandwidth for UDP traffic (protocol ID 17). See the preceding section titled, "Preventing heavy data traffic from impacting telephone calls.

3 Provision the IP set with the corporate call server address.

4 On the PC, install Contivity Client Software, and configure it with the PC user account information.

Inter-Operability With Third-Party Routers

VPN Connections With Cisco Routers

When establishing a VPN Client tunnel or Branch Office Tunnel between the Business Secure Router and a Cisco router, the following configuration rules should be followed:

1 Ensure that the WAN IP of the BSR222/252 router and the Cisco router are not in the same subnet.

2 Configure the connection to use DES Encryption and MD5 Authentication.

Chapter 5
System screens

This chapter provides information on the System screens.

System overview

This section provides background information on features that you cannot configure in the Wizard.

DNS overview

There are three places where you can configure DNS (Domain Name System) setup on the Business Secure Router.

Use the **System General** screen to configure the Business Secure Router to use a DNS server to resolve domain names for Business Secure Router system features like VPN, DDNS, and the time server.

Use the **LAN IP** screen to configure the DNS server information that the Business Secure Router sends to the DHCP client devices on the LAN.

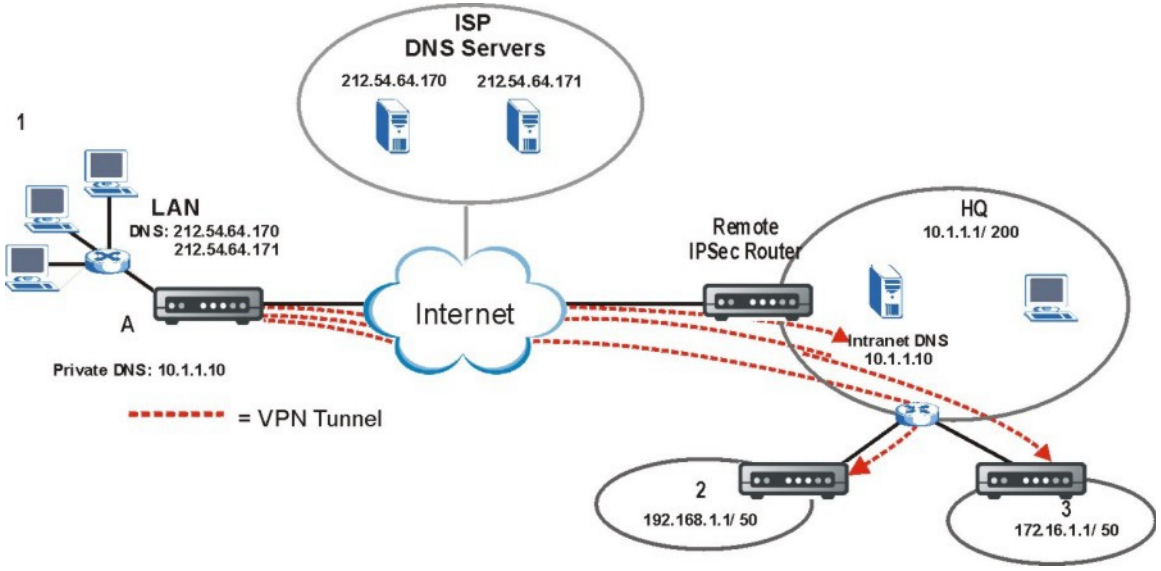
Use the **Remote Management DNS** screen to configure the Business Secure Router to accept or discard DNS queries.

Private DNS server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP because these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

Figure 13 depicts an example where three VPN tunnels are created from Business Secure Router A; one to branch office **2**, one to branch office **3,** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the Business Secure Router at branch office **1** uses the Intranet DNS server in headquarters.

Figure 13 Private DNS server example



Note: If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 14 System general setup

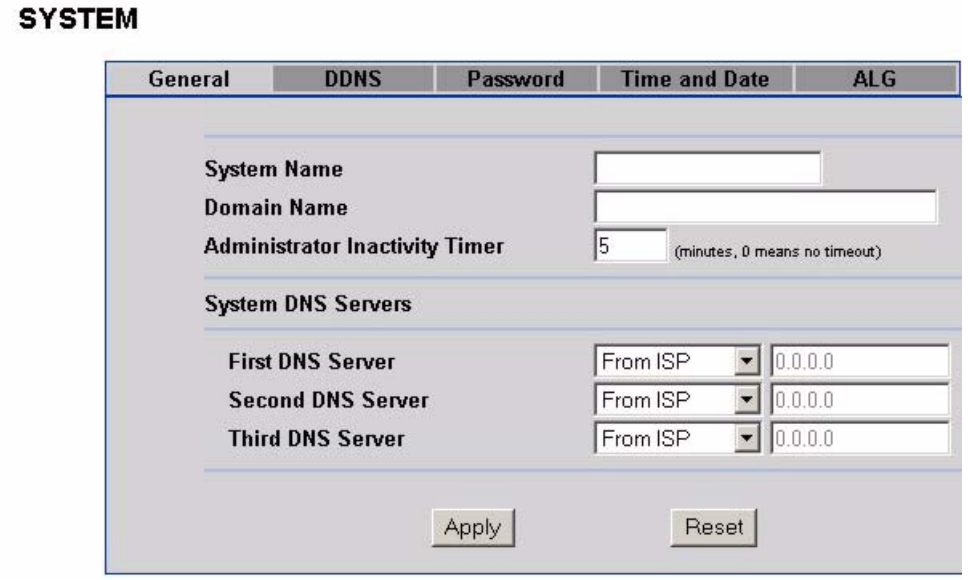


Table 8 describes the fields in Figure 14.

Table 8 System general setup

Label	Description
System Name	Choose a descriptive name for identification purposes. Nortel recommends that you enter your computer name in this field. This name can be up to 30 alphanumeric characters long. Spaces, dashes (-) and underscores (_) are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP assigns a domain name via DHCP. The domain name entered by you is given priority over the ISP-assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the WebGUI or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts can have security risks. A value of 0 means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Table 8 System general setup

Label	Description
System DNS Servers (if applicable)	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Business Secure Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Business Secure Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Business Secure Router has a fixed WAN IP address, **From ISP** changes to **None** after you click **Apply**. If you chose **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after you click **Apply**. Select **User-Defined** if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. A **User-Defined** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **User-Defined** entry changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. Select **Private DNS** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in the **LAN IP** screen to use **DNS Relay**. You must also configure a VPN branch office rule since the Business Secure Router uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the Business Secure Router as a local IP address and the IP address of the DNS server as a remote IP address. A **Private DNS** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **Private DNS** entry changes to **None** after you click **Apply**.

Dynamic DNS

With Dynamic DNS, you can update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (as in NetMeeting or CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance, myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives can always call you even if they don't know your IP address.

First of all, you must register a dynamic DNS account with, for example www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that still wants a domain name. The Dynamic DNS service provider gives you a password or key.

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to use, for example, www.yourhost.dyndns.org and still reach your host name.

Configuring Dynamic DNS

Note: If you have a private WAN IP address, you cannot use Dynamic DNS.

To change your Business Secure Router's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen illustrated in Figure 15 appears.

Figure 15 DDNS

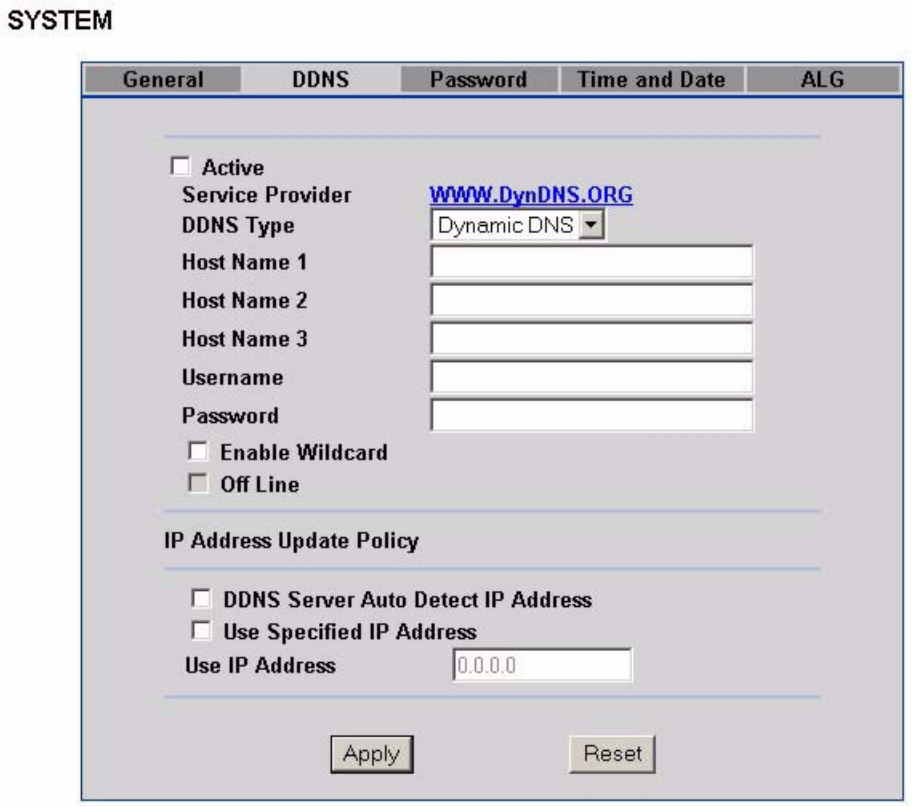


Table 9 describes the fields in Figure 15.

Table 9 DDNS

Label	Description
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (,).
User	Enter your username (up to 31 characters).

Table 9 DDNS

Label	Description
Password	Enter the password associated with your username (up to 31 characters).
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
DDNS Server Auto Detect IP Address	Select this option only when there are one or more NAT routers between the Business Secure Router and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. **Note:** The DDNS server not be able to detect the proper IP address if there is an HTTP proxy server between the Business Secure Router and the DDNS server.
Use Specified IP Address	Select this option to update the IP address of the host names to the IP address specified below. Use this option if you have a static IP address.
Use IP Address	Enter the IP address if you select the **User Specify** option.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to return to the previously saved settings.

Configuring Password

To change the password of your Business Secure Router (recommended), click **SYSTEM**, then the **Password** tab. The screen illustrated in Figure 16 appears. In this screen, you can change password of the Business Secure Router.

Figure 16 Password

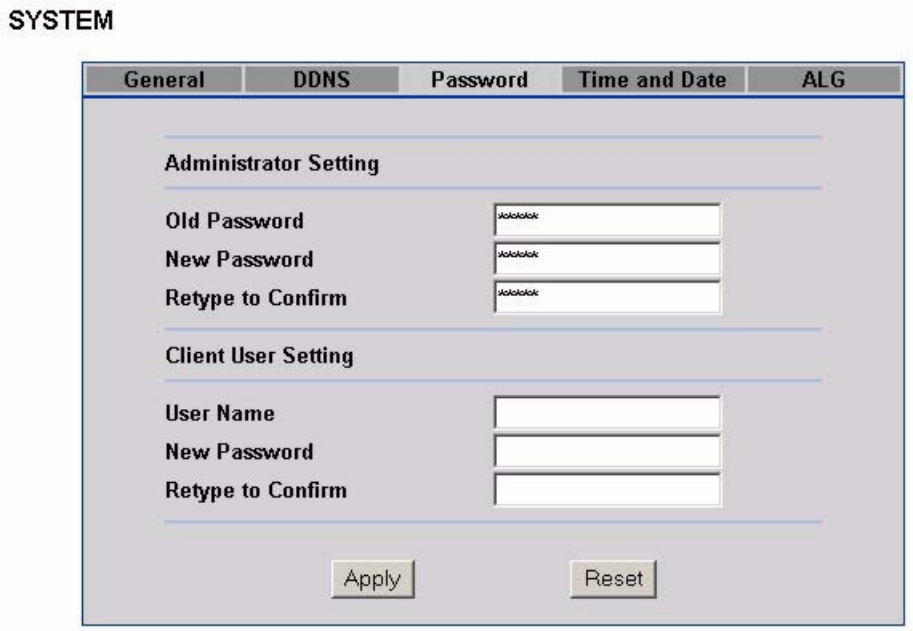


Table 10 describes the fields in Figure 16.

Table 10 Password

Label	Description
Administrator Setting	The administrator can access and configure all of the Business Secure Router's features.
Old Password	Type your existing system administrator password (PlsChgMe! is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.

Table 10 Password

Label	Description
Client User Setting	The client user is the person who uses the Business Secure Router's Contivity Client VPN tunnel. The client user can do the following: • Configure the **WAN ISP** and **IP** screens. • Configure the VPN Contivity Client settings (except the **Advanced** screen's exclusive use mode for client tunnel and MAC address allowed settings). • View the SA monitor. • Configure the **VPN Global Setting** screen. • View logs. • View the **Maintenance Status** screen. • Use the **Maintenance F/W Upload** and **Restart** screens.
User Name	Type a username for the client user (up to 31 characters).
New Password	Type a password for the client user (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype the client user password for confirmation.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Predefined NTP time server list

The Business Secure Router uses the predefined list of NTP time servers listed in Table 11 if you do not specify a time server or if it cannot synchronize with the time server you specified.

The Business Secure Router can use this predefined list of time servers regardless of the Time Protocol you select.

When the Business Secure Router uses the predefined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Business Secure Router goes through the rest of the list in order from the first one tried until either it is successful or all the predefined NTP time servers have been tried.

Table 11 Default Time Servers

a.ntp.alphazed.net
ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

Configuring Time and Date

To change your Business Secure Router's time and date, click **SYSTEM**, and then **Time and Date**. The screen in Figure 17 appears. Use this screen to configure the Business Secure Router's time based on your local time zone.

Figure 17 Time and Date

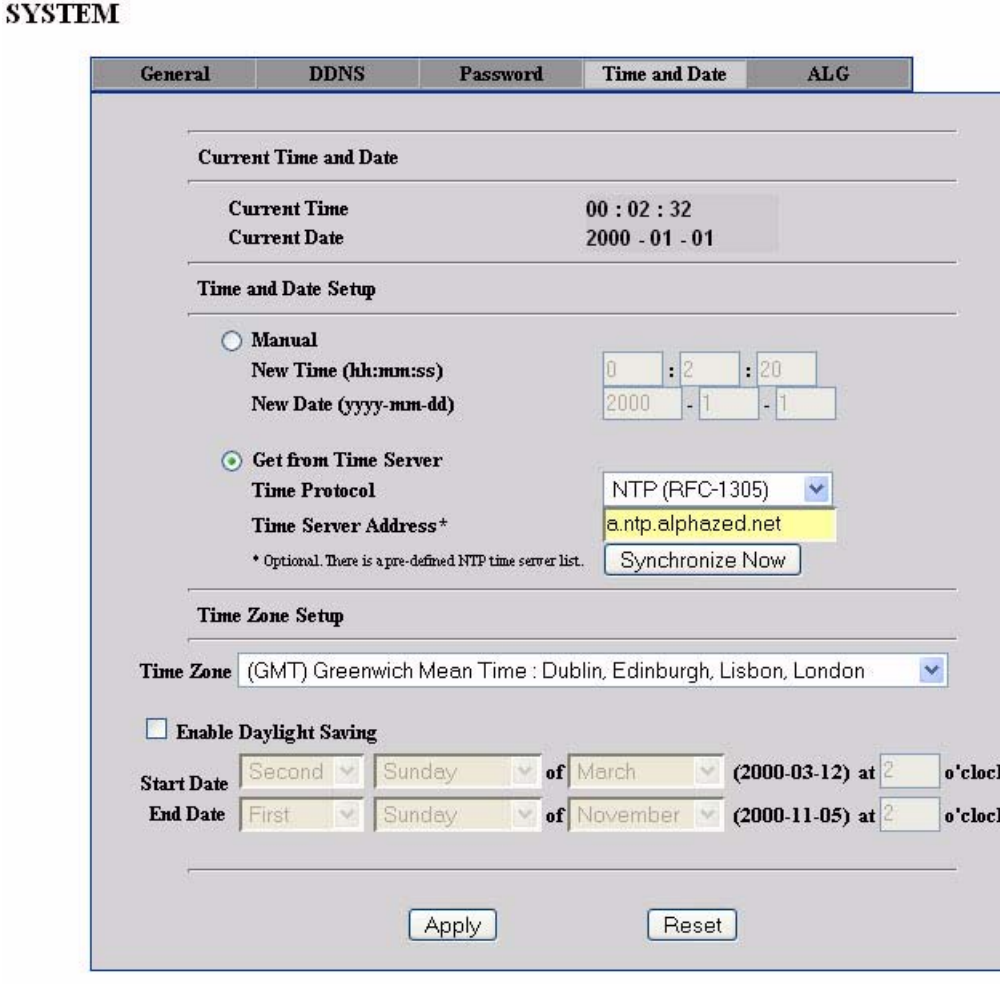


Table 12 describes the fields in Figure 17.

Table 12 Time and Date

Label	Description
Current Time and Date	
Current Time	This field displays the time on your Business Secure Router. Each time you reload this page, the Business Secure Router synchronizes the time with the time server.
Current Date	This field displays the date on your Business Secure Router. Each time you reload this page, the Business Secure Router synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. After you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. After you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the Business Secure Router get the time and date from the time server that you specified.
Time Protocol	Select the time service protocol that your time server sends when you turn on the Business Secure Router. Not all time servers support all protocols, so you need to check with your ISP or network administrator or use trial and error to find a protocol that works. The main difference between the protocols is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the Business Secure Router get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address).

Table 12 Time and Date

Label	Description
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you select **Enable Daylight Saving**. The **o'clock** field uses the 24-hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 a.m. local time. So, in the United States, select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 a.m. GMT or UTC). So, in the European Union, select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany, for instance, type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you select **Enable Daylight Saving**. The **o'clock** field uses the 24-hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 a.m. local time. So, in the United States, select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 a.m. GMT or UTC). So, in the European Union, select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

ALG

With Application Layer Gateway (ALG), applications can pass through NAT and the firewall. You must also configure NAT and firewall rules depending upon the type of access you want to allow.

Note: You must enable the FTP, H.323 or SIP ALG in order to use bandwidth management on that application.

Configuring ALG

To change the ALG settings of your Business Secure Router, click **SYSTEM** and then **ALG.** The screen appears as shown in Figure 18.

Figure 18 ALG

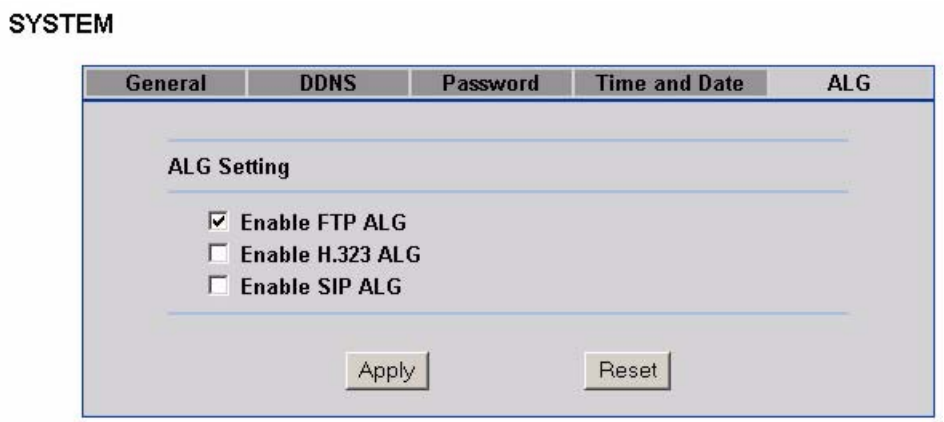


Table 13 describes the labels in Figure 18.

Table 13 ALG

Label	Description
Enable FTP ALG	Select this check box to allow FTP (File Transfer Protocol) to send and receive files through the Business Secure Router.
Enable H.323 ALG	Select this check box to allow applications using H.323 to go through the Business Secure Router. H.323 is an application layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. H.323 is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol. The H.323 ALG does not support H.323 Gatekeeper.
Enable SIP ALG	Select this check box to allow SIP (Session Initiation Protocol) applications to go through the Business Secure Router. The Session Initiation Protocol (SIP) is an application layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol. To avoid retranslating the SIP device's IP address, do not use the SIP ALG with a SIP device that is using STUN (Simple Traversal of User Datagram Protocol (UDP) through NAT).
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 6
LAN screens

This chapter describes how to configure LAN settings.

LAN overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, configure RIP and multicast settings, and partition your physical network into logical networks.

DHCP setup

Using DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132), individual clients can obtain TCP/IP configuration at start-up from a server. You can configure the Business Secure Router as a DHCP server or disable it. When configured as a server, the Business Secure Router provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be configured manually.

IP pool setup

The Business Secure Router is preconfigured with a pool of IP addresses for the DHCP clients (DHCP Pool). Do not assign static IP addresses from the DHCP pool to your LAN computers.

DNS servers

Use the **LAN IP** screen to configure the DNS server information that the Business Secure Router sends to the DHCP client devices on the LAN.

LAN TCP/IP

The Business Secure Router has built in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Factory LAN defaults

The LAN parameters of the Business Secure Router are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 126 client IP addresses starting from 192.168.1.2.

These parameters work for the majority of installations. If your ISP gives you explicit DNS server addresses, read the embedded WebGUI help regarding which fields need to be configured.

RIP setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the Business Secure Router broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the Business Secure Router sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

Multicast

Traditionally, IP packets are transmitted in one of two ways—Unicast (1 sender-1 recipient) or Broadcast (1 sender-everybody on the network). Multicast delivers IP packets to a group of hosts on the network—not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of *Internet Group Management Protocol* (RFC 2236). The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Business Secure Router supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Business Secure Router queries all directly connected networks to gather group membership. After that, the Business Secure Router periodically updates this information. IP multicasting can be enabled or disabled on the Business Secure Router LAN, WAN or both interfaces in the WebGUI (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Configuring IP

Click **LAN** to open the **IP** screen.

Figure 19 LAN IP

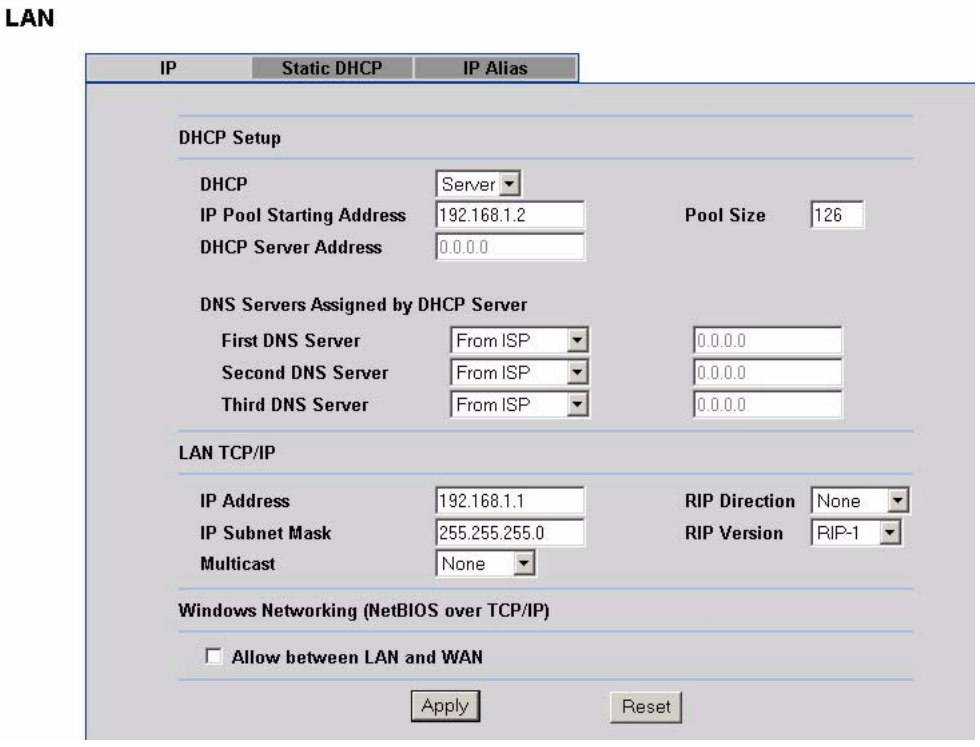


Table 14 describes the fields in Figure 19.

Table 14 LAN IP

Label	Description
DHCP Server	With DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) individual clients (workstations) can obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the Business Secure Router provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields. Select **Relay** to have the Business Secure Router forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field. Select **None** to stop the Business Secure Router from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.2.
Pool Size	This field specifies the size, or count, of the IP address pool. The default is 126.
DNS Servers Assigned by DHCP Server	The Business Secure Router passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Business Secure Router only passes this information to the LAN DHCP clients when you select the **DHCP Server** check box. When you clear the **DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 14 LAN IP

Label	Description
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Business Secure Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **DNS Relay** to have the Business Secure Router act as a DNS proxy. The Business Secure Router's LAN IP address displays in the field to the right (read-only). The Business Secure Router tells the DHCP clients on the LAN that the Business Secure Router itself is the DNS server. When a computer on the LAN sends a DNS query to the Business Secure Router, the Business Secure Router forwards the query to the Business Secure Router's system DNS server (configured in the **SYSTEM General** screen) and relays the response to the computer. You can only select **DNS Relay** for one of the three servers. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
LAN TCP/IP	
IP Address	Type the IP address of your Business Secure Router in dotted decimal notation (192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Business Secure Router automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Business Secure Router 255.255.255.0.
RIP Direction	With RIP (Routing Information Protocol, RFC 1058 and RFC 1389) a router can exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the Business Secure Router broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **None** is the default.

Table 14 LAN IP

Label	Description
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Business Secure Router sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so does not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of *Internet Group Management Protocol* (RFC 2236).
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. This field does the same as the **Allow between WAN and LAN** field in the **WAN IP** screen. Enabling one automatically enables the other.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Static DHCP

With Static DHCP, you can assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your Business Secure Router's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown in Figure 20.

Figure 20 Static DHCP

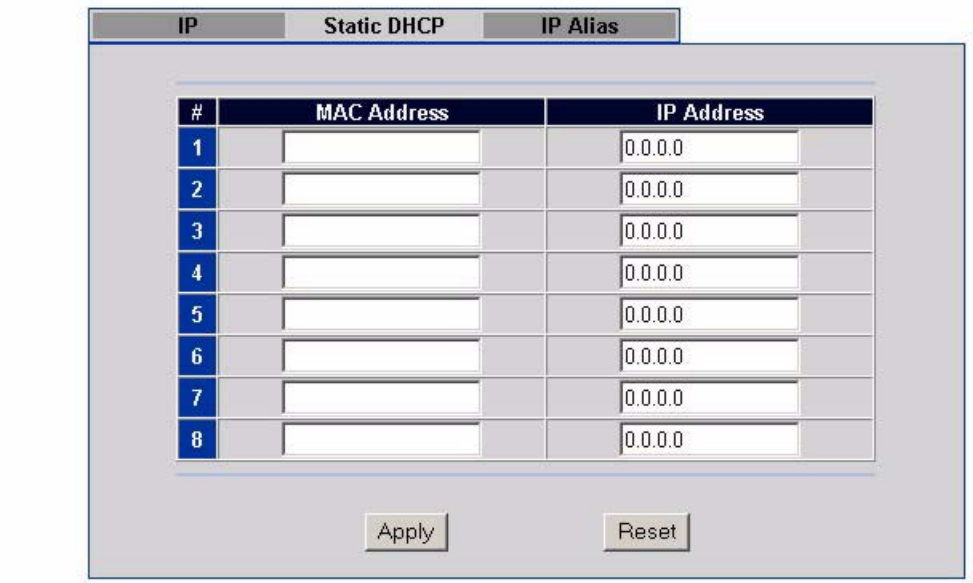


Table 15 describes the fields in Figure 20.

Table 15 Static DHCP

Label	Description
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.

Table 15 Static DHCP

Label	Description
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring IP Alias

With IP Alias, you can partition a physical network into different logical networks over the same Ethernet interface. The Business Secure Router supports three logical LAN interfaces via its single physical Ethernet interface with the Business Secure Router itself as the gateway for each LAN network.

Note: Make sure that the subnets of the logical networks do not overlap.

To change the IP Alias settings of your Business Secure Router, click **LAN**, then the **IP Alias** tab. The screen appears as shown in Figure 21.

Figure 21 IP Alias

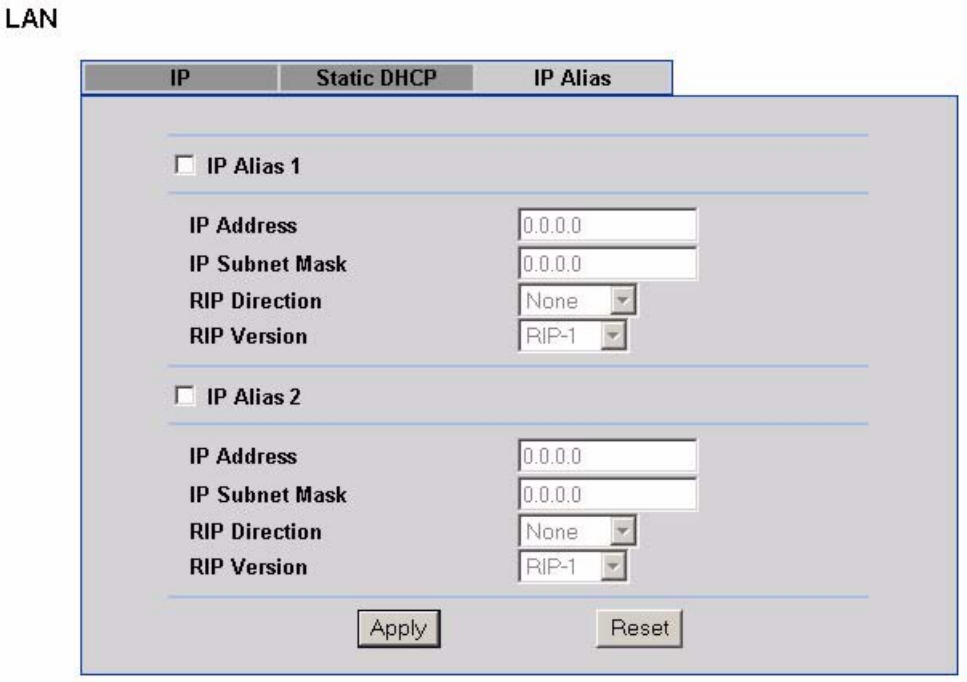


Table 16 describes the fields in Figure 21.

Table 16 IP Alias

Label	Description
IP Alias 1,2	Select the check box to configure another LAN network for the Business Secure Router.
IP Address	Enter the IP address of your Business Secure Router in dotted decimal notation.
IP Subnet Mask	Your Business Secure Router automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Business Secure Router.

Table 16 IP Alias

Label	Description
RIP Direction	With RIP (Routing Information Protocol, RFC1058 and RFC 1389), a router can exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/ **None**. When set to **Both** or **Out Only**, the Business Secure Router broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Business Secure Router sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on nonrouter machines because they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 7
WAN screens

This chapter describes how to configure WAN settings.

WAN Overview

This section provides background information on features that you cannot configure in the Wizard.

7.1 TCP/IP Priority (Metric)

The metric represents the cost of transmission. A router determines the best route for transmission by choosing a path with the lowest cost. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number must be between 1 and 15; a number greater than 15 means the link is down. The smaller the number, the lower the cost.

1. The metric sets the priority for the routes of the Business Secure Router to the Internet. Each route must have a unique metric.
2. The priority of the WAN port route must always be higher than the dial backup and traffic redirect route priorities.

If the WAN port route has a metric of 1 and the traffic redirect route has a metric of 2 and dial backup route has a metric of 3, then the WAN port route acts as the primary default route. If the WAN port route fails to connect to the Internet, the Business Secure Router tries the traffic redirect route next. In the same manner, the Business Secure Router uses the dial backup route if the traffic redirect route also fails.

The dial backup or traffic redirect routes cannot take priority over the WAN routes.

Configuring Route

Click **WAN** to open the **Route** screen.

Figure 22 WAN: Route

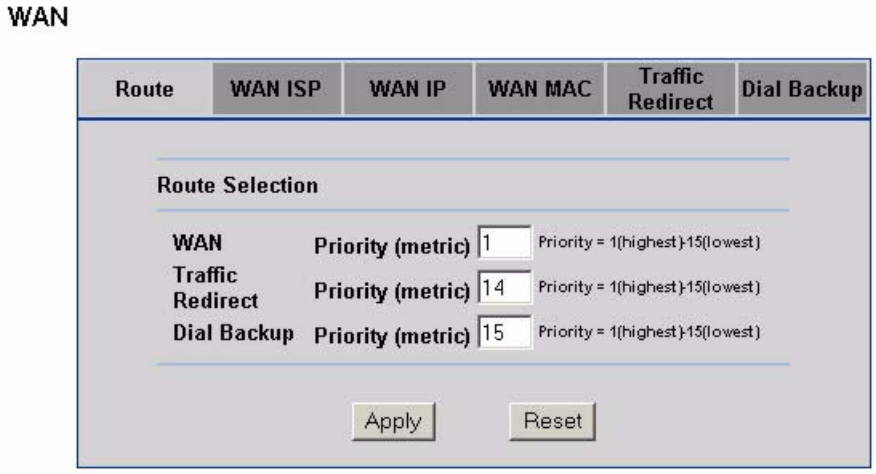


Table 17 describes the fields in Figure 22.

Table 17 WAN: Route

Label	Description
WAN Traffic Redirect Dial Backup	The default WAN connection is 1 as your broadband connection via the WAN port must always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all Business Secure Router models): You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type 14 in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of 15).

Table 17 WAN: Route

Label	Description
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN ISP

To change your Business Secure Router's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

Ethernet Encapsulation

The screen shown in Figure 23 is for Ethernet encapsulation.

Figure 23 Ethernet Encapsulation

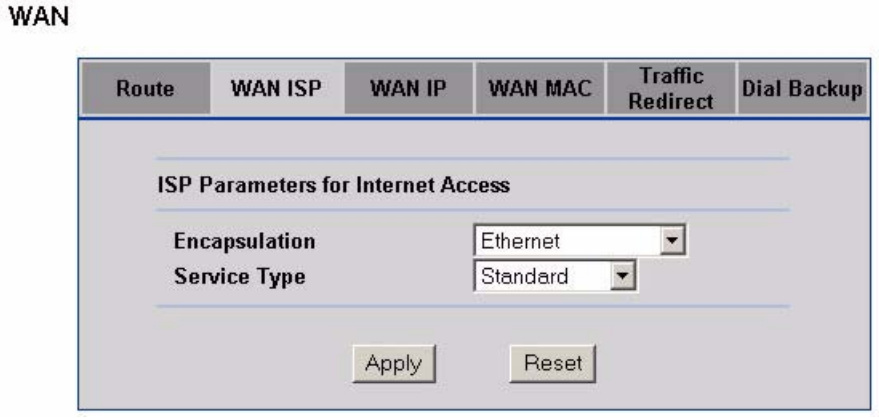


Table 18 describes the fields in Figure 23.

Table 18 Ethernet Encapsulation

Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (Road Runner Telstra authentication method), **RR-Manager** (Road Runner Manager authentication method) or **RR-Toshiba** (Road Runner Toshiba authentication method). The following fields do not appear with the **Standard** service type.
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the username.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

PPPoE Encapsulation

The Business Secure Router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (for example, DSL, cable, or wireless) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example, Radius). PPPoE provides a logon and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This makes it easy for the service provider to create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Business Secure Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Business Secure Router does that part of the task. Furthermore, with NAT, all of the computers on the LAN have access.

The screen shown in Figure 24 is for **PPPoE** encapsulation.

Figure 24 PPPoE Encapsulation

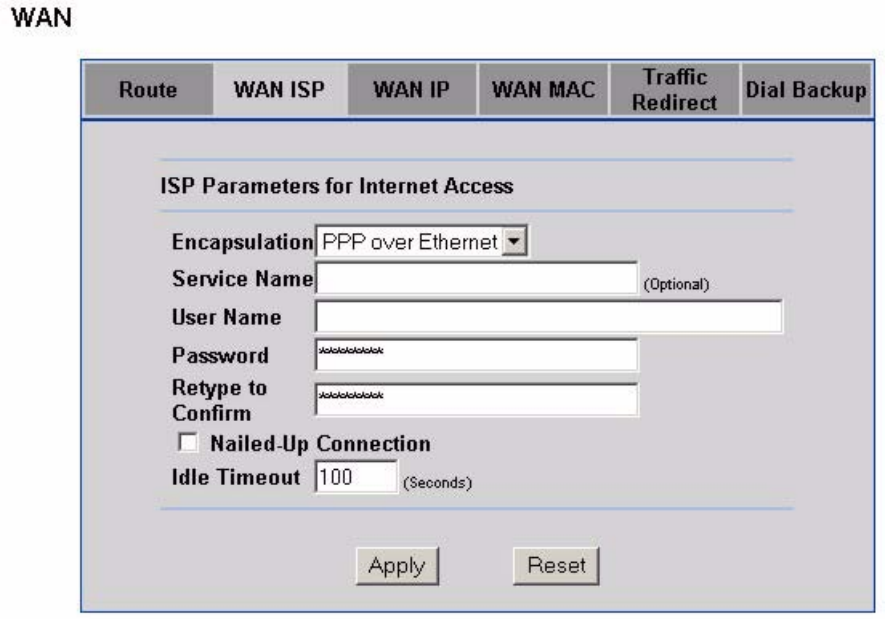


Table 19 describes the fields in Figure 24.

Table 19 PPPoE Encapsulation

Label	Description
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (for example, DSL, cable, or wireless) connection. Operationally, PPPoE saves significant effort for both the end user and ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the computers on the LAN have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the username.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that makes secure transfer of data from a remote client to a private server possible by creating a Virtual Private Network (VPN) using TCP/IP based networks.

PPTP supports on-demand, multiprotocol and virtual private networking over public networks, such as the Internet.

The screen shown in Figure 25is for **PPTP** encapsulation.

Figure 25 PPTP Encapsulation

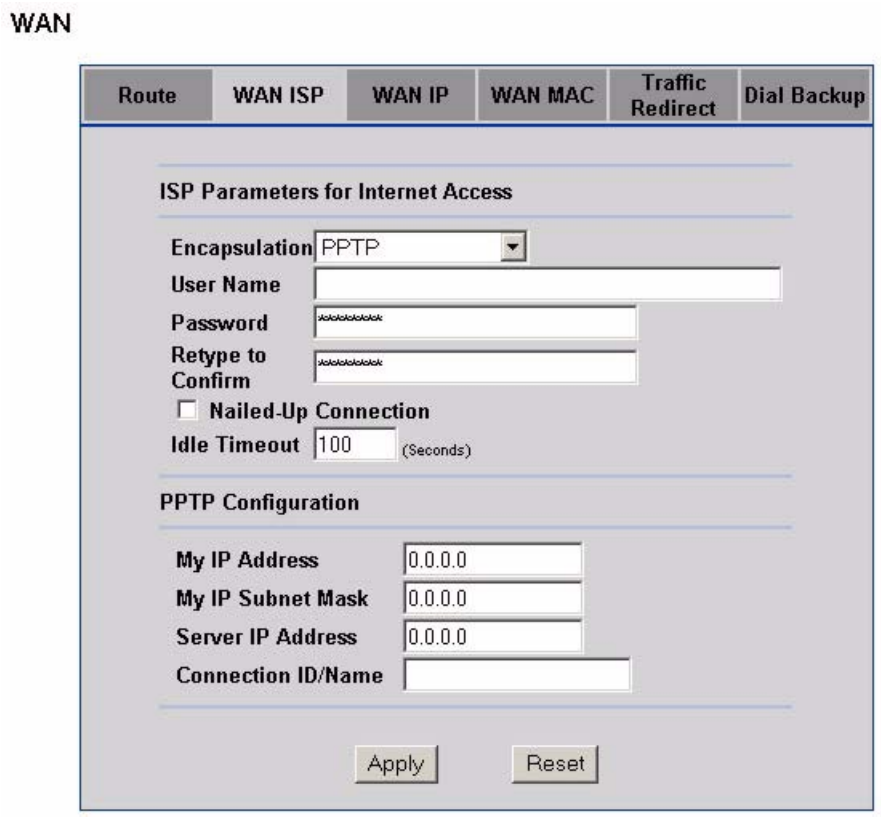


Table 20 describes the fields in Figure 25.

Table 20 PPTP Encapsulation

Label	Description
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that makes secure transfer of data from a remote client to a private server possible by creating a Virtual Private Network (VPN) using TCP/IP based networks. PPTP supports on-demand, multiprotocol, and virtual private networking over public networks, such as the Internet. The Business Secure Router supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the username given to you by your ISP.

Table 20 PPTP Encapsulation

Label	Description
Password	Type the password associated with the username.
Nailed up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time, in seconds, that elapses before the Business Secure Router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your Business Secure Router automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Business Secure Router.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Service type

The screen shown in Figure 26 is for **RR- Service type**.

Figure 26 RR Service type

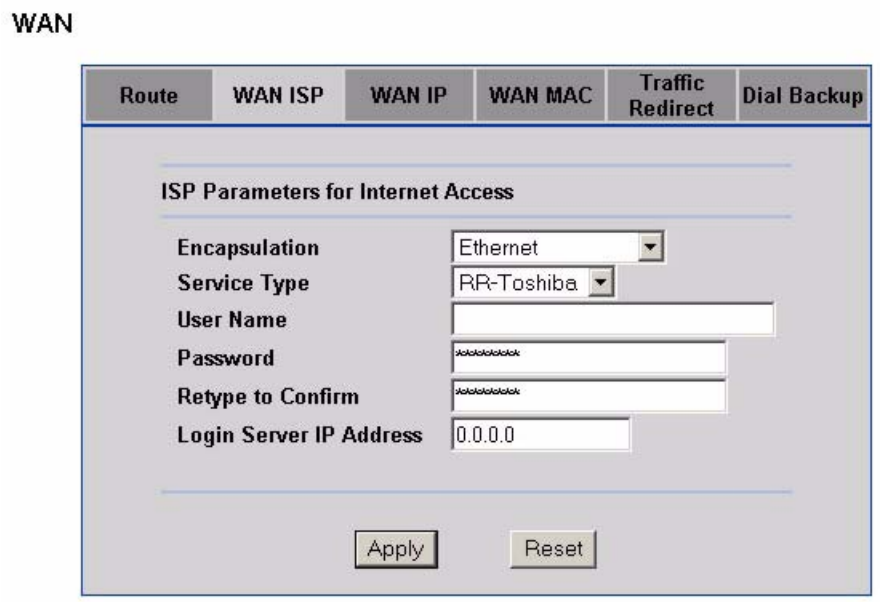


Table 21 describes the fields in Figure 26.

Table 21 RR Service Type

Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from **Standard**, **RR-Toshiba** (Road Runner Toshiba authentication method), **RR-Manager** (Road Runner Manager authentication method) or **RR-Telstra**. Choose a Road Runner service type if your ISP is Time Warner's Road Runner; otherwise choose **Standard**.
User Name	Enter the username given to you by your ISP.
Password	Enter the password associated with the username.
Login Server IP Address	The Business Secure Router finds the Road Runner Server IP address if this field is left blank. If it does not, you must enter the authentication server IP address.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN IP

To change the WAN IP settings of your Business Secure Router, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP** (**Default**); otherwise click **Use fixed IP Address** and enter the IP address in the field **My WAN IP Address**.

Figure 27 WAN: IP

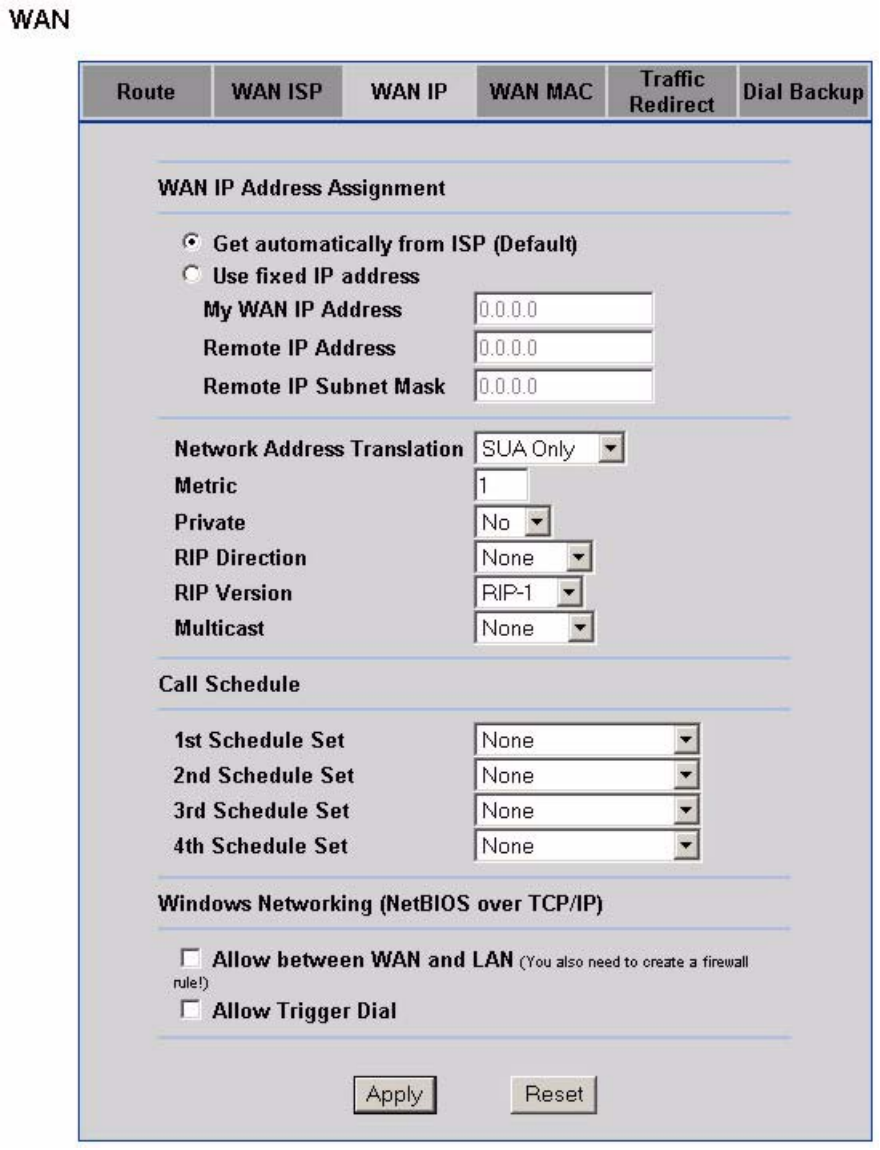


Table 22 describes the fields in this Figure 27.

Table 22 WAN: IP

Label	Description
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option if your ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Network Address Translation	With Network Address Translation (NAT), the router translations an Internet protocol address used within one network (for example, a private IP address used in a local network) to a different IP address known within another network (for example, a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. After you select **Full Feature,** you must configure at least one address-mapping set.
Metric (PPPoE and PPTP only)	This field sets this route's priority among the routes the Business Secure Router uses. The metric represents the cost of transmission. A router determines the best route for transmission by choosing a path with the lowest cost. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number must be between 1 and 15; a number greater than 15 means the link is down. The smaller the number, the lower the cost.
Private (PPPoE and PPTP only)	This parameter determines if the Business Secure Router includes the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node is propagated to other hosts through RIP broadcasts.

Table 22 WAN: IP

Label	Description
RIP Direction	With RIP (Routing Information Protocol), a router can exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Business Secure Router broadcasts its routing table periodically. When set to **Both** or **In Only**, the Business Secure Router incorporates RIP information that it receives. When set to **None**, the Business Secure Router does not send any RIP packets and ignores any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Business Secure Router sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of *Internet Group Management Protocol* (RFC 2236).
Call Schedule (PPPoE and PPTP encapsulation)	Apply call schedule sets for this remote node. Use the **Call Schedule** screens to configure call schedule sets (see Chapter 21, “Call scheduling screens,” on page 385).
Windows Networking (NetBIOS over TCP/IP):	Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services, such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

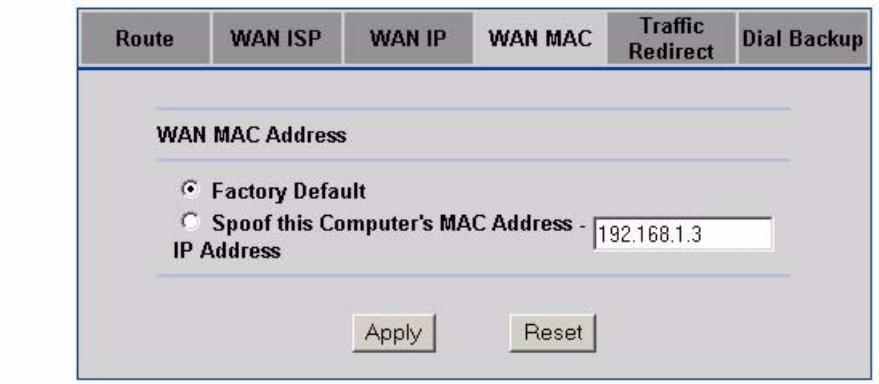
Table 22 WAN: IP

Label	Description
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you must also enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. This field does the same as the **Allow between LAN and WAN** field in the **LAN IP** screen. Enabling one automatically enables the other.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN MAC

To change the WAN MAC settings of your Business Secure Router, click **WAN**, then the **WAN MAC** tab. The screen appears as shown in Figure 28.

Figure 28 MAC Setup



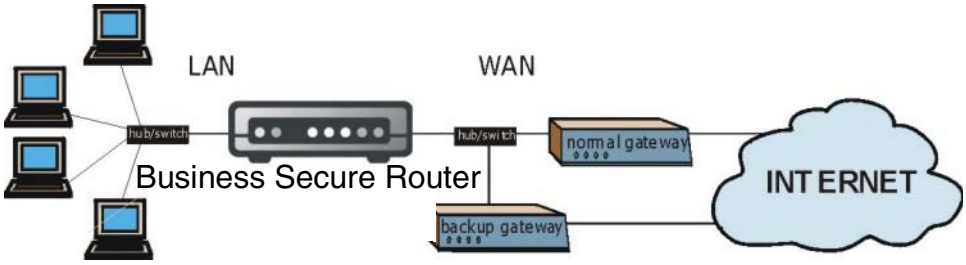
Using the MAC address screen, users can configure the MAC address of the WAN port by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC address you are cloning. After it is successfully configured, the address is copied to the rom file (configuration file). It does not change unless you change the setting or upload a different ROM file.

Traffic redirect

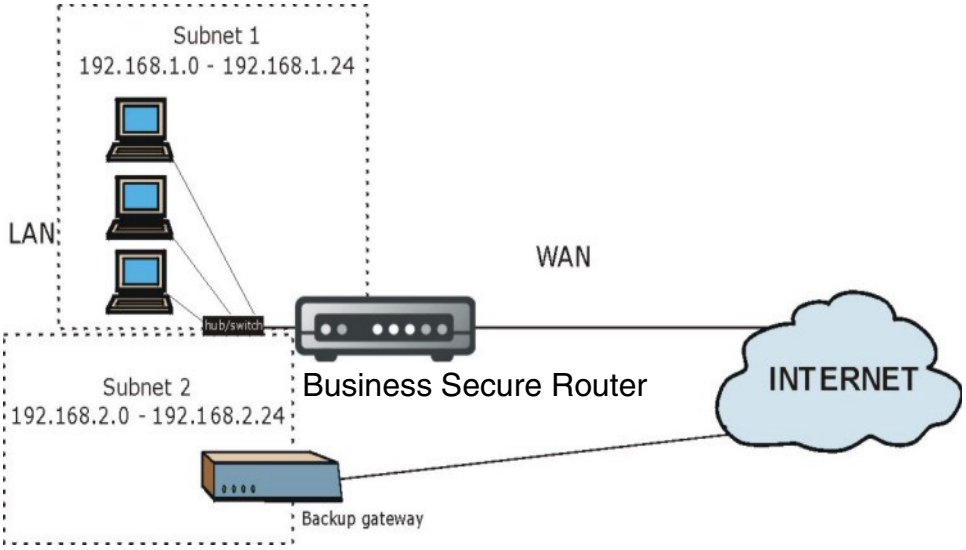
Traffic redirect forwards WAN traffic to a backup gateway when the Business Secure Router cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the Business Secure Router still provides firewall protection. This feature is not available on all models.

Figure 29 Traffic Redirect WAN Setup



The network topology illustrated in Figure 30 avoids triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the Business Secure Router itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in Figure 30) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/Business Secure Router firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 30 Traffic Redirect LAN Setup



Configuring Traffic Redirect

To change your Business Secure Router's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown in Figure 31.

Figure 31 Traffic Redirect

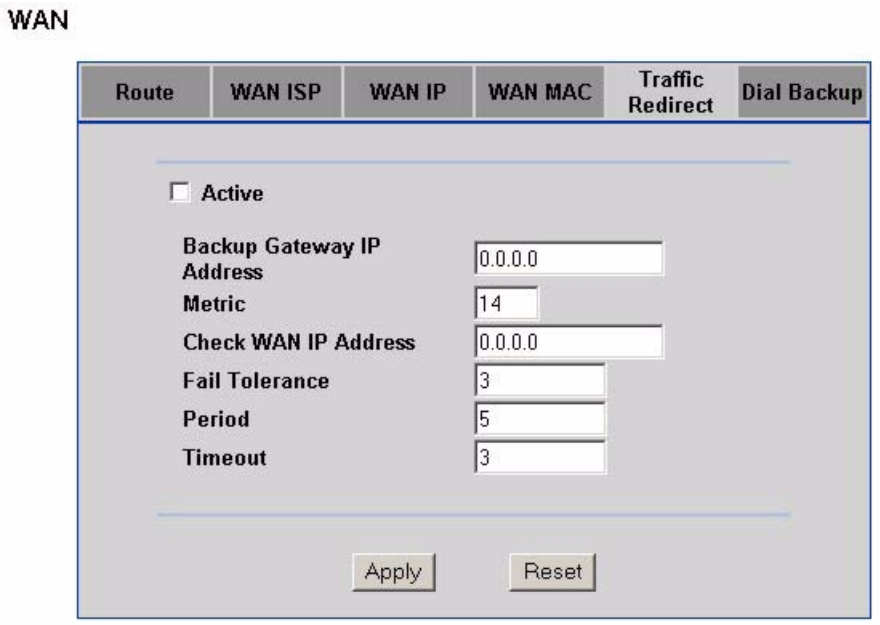


Table 23 describes the fields in Figure 31.

Table 23 Traffic Redirect

Label	Description
Active	Select this check box to have the Business Secure Router uses traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The Business Secure Router automatically forwards traffic to this IP address if the Business Secure Router's Internet connection terminates.
Metric	This field sets this route's priority among the routes the Business Secure Router uses. The metric represents the cost of transmission. A router determines the best route for transmission by choosing a path with the lowest cost. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number must be between 1 and 15. A number greater than 15 means the link is down. The smaller the number, the lower the cost.

Table 23 Traffic Redirect

Label	Description
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the Business Secure Router uses the default gateway IP address. Configure this field to test your Business Secure Router's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type 0.0.0.0 to configure the Business Secure Router to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Enter the number of times Business Secure Router will attempt to connect to the Internet before traffic is forwarded to the backup gateway.
Period (sec)	Type the number of seconds for the Business Secure Router to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds for your Business Secure Router to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered down after the Business Secure Router times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Dial Backup

To change your Business Secure Router's Dial Backup settings, click **WAN**, then the **Dial Backup** tab. The screen appears as shown in Figure 32.

Figure 32 Dial Backup Setup

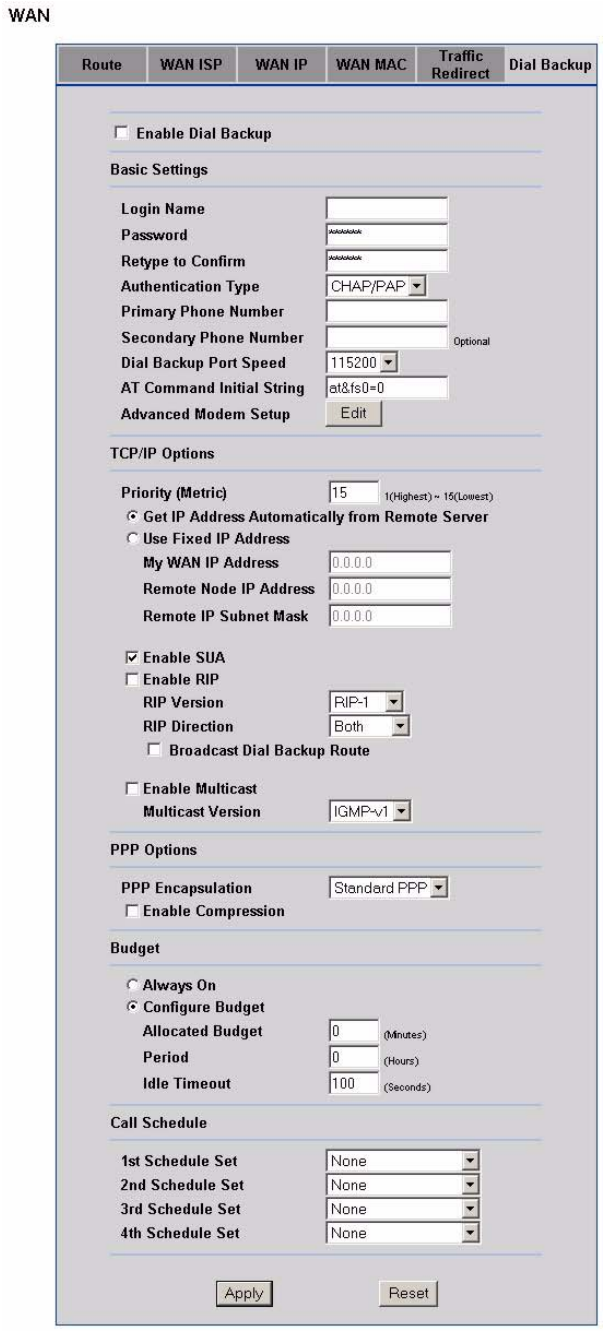


Table 24 describes the fields in Figure 32.

Table 24 Dial Backup Setup

Label	Description
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
Login Name	Type the logon name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again in this field.
Authentication Type	Use the drop-down list to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Business Secure Router accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Business Secure Router accepts CHAP only. **PAP** - Your Business Secure Router accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Business Secure Router dials the Secondary Phone number, if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9 600, 19 200, 38 400, 57 600, 115 200 or 230 400 b/s.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click this button to display the **Advanced Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Priority (Metric)	This field sets this route's priority among the three routes the Business Secure Router uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Get IP Address Automatically from Remote Server	Type the logon name assigned by your ISP for this remote node.

Table 24 Dial Backup Setup

Label	Description
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address and then enter the IP address in the following field.
My WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address, if you do not know it. Type your WAN IP address here, if you know it (static). This is the address assigned to your local Business Secure Router, not the remote router.
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask, if you do not know it. Type the remote gateway's subnet mask here, if you know it (static).
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address, if you do not know it. Type the remote gateway's IP address here, if you know it (static).
Enable SUA	Using Network Address Translation (NAT), the router translates an Internet protocol address used within one network to a different IP address known within another network. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Business Secure Router uses Address Mapping Set 255. Clear this option to disable NAT.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Business Secure Router sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines because they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Table 24 Dial Backup Setup

Label	Description
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Business Secure Router broadcasts its routing table periodically. When set to **Both** or **In Only**, the Business Secure Router incorporates RIP information that it receives.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. For more information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of *Internet Group Management Protocol* (RFC 2236).
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget is reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the Business Secure Router to the remote node) for the Business Secure Router to wait before it automatically disconnects the dial backup connection. This option applies only when the Business Secure Router initiates the call. The dial backup connection never times out if you set this field to 0 (it is the same as selecting **Always On**).
Call Schedule Sets	Specify call schedule sets to use on the dial backup connection. The call schedule sets must already be configured (see Chapter 21, “Call scheduling screens,” on page 385).

Table 24 Dial Backup Setup

Label	Description
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Advanced Modem Setup

AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

For ISDN lines, there are many more protocols and operational modes. Consult the documentation of your TA. You need additional commands in both Dial and Init strings.

DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. If the **Drop DTR When Hang Up** check box is selected, the Business Secure Router uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

Response Strings

The response strings tell the Business Secure Router the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; consult the documentation of your WAN device to find the correct tags.

Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen shown in Figure 33.

Note: Consult the manual of your WAN device connected to your dial backup port for specific AT commands.
Note:

Figure 33 Advanced Setup

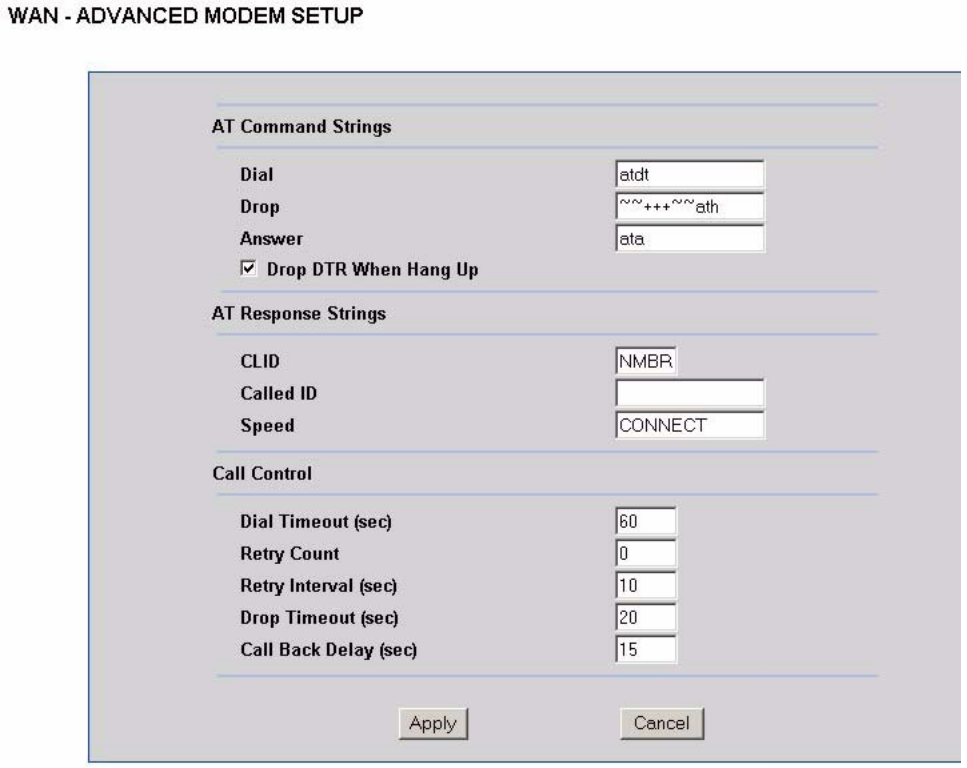


Table 25 describes the fields in Figure 33.

Table 25 Advanced Setup

Label	Description	Example
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt
Drop	Type the AT Command string to drop a call. ~ represents a one-second wait. For example, ~~~+++~~ath can be used if your modem has a slow response time.	~~+++~~ath
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the Business Secure Router drop the DTR (Data Terminal Ready) signal after the AT Command String: Drop is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Business Secure Router capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the Business Secure Router to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the Business Secure Router to retry a busy or no answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the Business Secure Router to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the Business Secure Router to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the Business Secure Router to wait between dropping a callback request call and dialing the corresponding callback call.	15

Table 25 Advanced Setup

Label	Description	Example
Apply	Click **Apply** to save your changes to the Business Secure Router.	
Reset	Click **Reset** to begin configuring this screen afresh.	

Chapter 8
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Business Secure Router.

NAT overview

NAT (Network Address Translation—NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network, is changed to a different IP address known within another network.

NAT definitions

Inside/outside denotes where a host is located relative to the Business Secure Router. For example, the computers of your subscribers are the inside hosts, while the Web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. Table 26 summarizes this information.

Table 26 NAT definitions

Term	Description
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT does

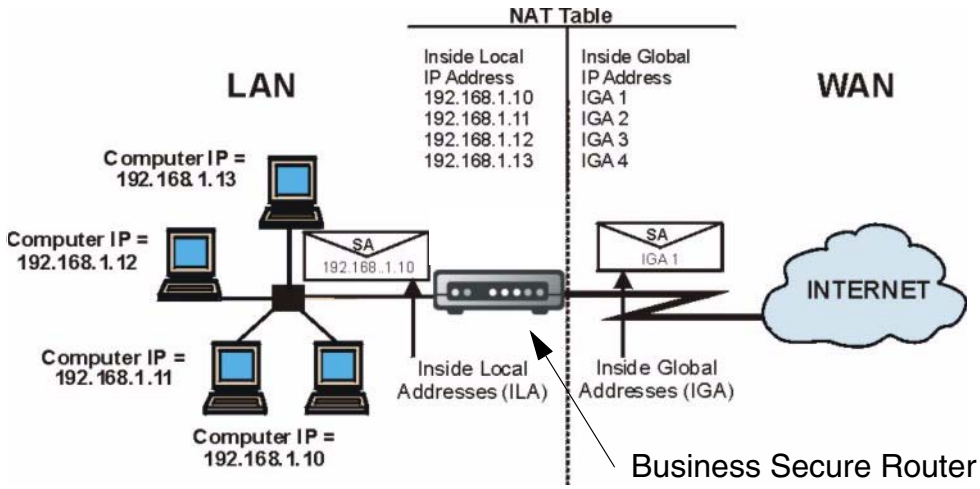
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a Telnet server) on your local network and make them accessible to the outside world. You can make designated servers on the LAN accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Business Secure Router filters out all incoming inquiries, thus preventing intruders from probing your network. For more information about IP address translation, refer to *The IP Network Address Translator (NAT)* (RFC 1631).

How NAT works

Each packet has two addresses–a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Business Secure Router keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored, as illustrated in Figure 34.

Figure 34 How NAT works



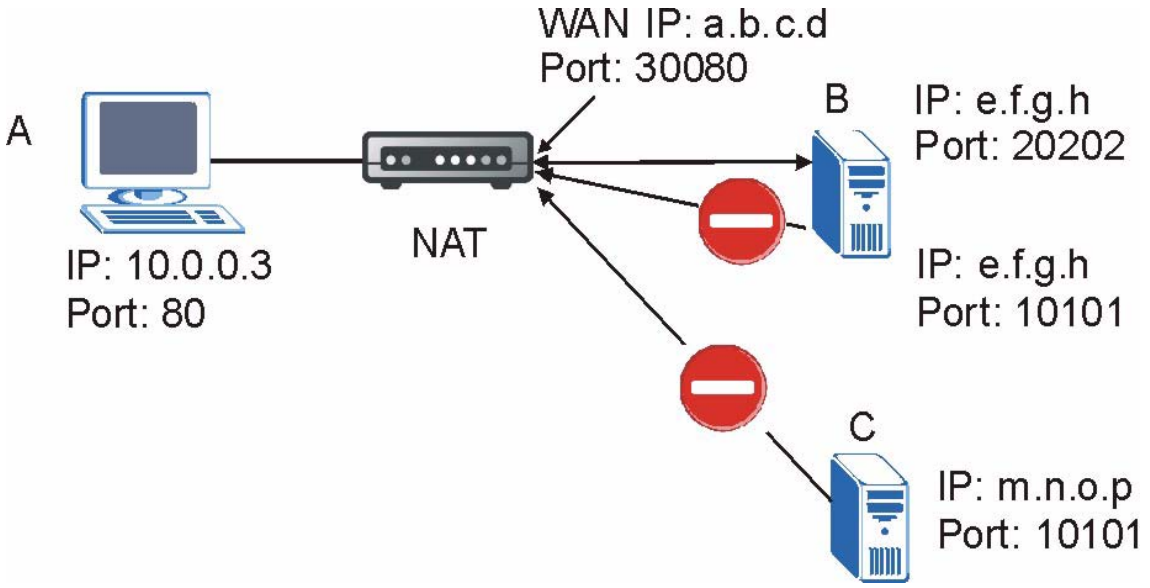
Port Restricted Cone NAT

The Business Secure Router uses port restricted cone NAT.

Port restricted cone NAT maps all requests from the same private IP address and port to the same public IP address and port. A host on the Internet can only send a packet to the private IP address and port if the private IP address and port has previously sent a packet to that host's IP address and port.

In Figure 35, B can send packets, with source IP address e.f.g.h and port 20202 to A because A previously sent a packet to IP address e.f.g.h and port 20202. B cannot send packets, with source IP address e.f.g.h and port 10101 to A because A has not sent a packet to IP address e.f.g.h and port 10101.

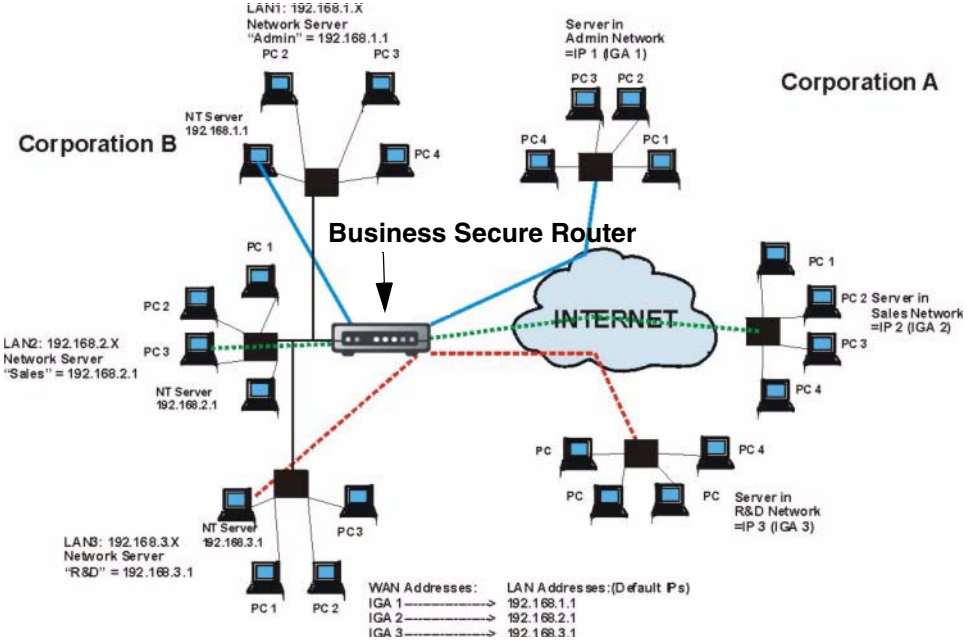
Figure 35 Port Restricted Cone NAT



NAT application

Figure 36 illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Business Secure Router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 36 NAT application with IP Alias



NAT mapping types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the Business Secure Router maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the Business Secure Router maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the Single User Account feature (the SUA Only option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the Business Secure Router maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the Business Secure Router maps each local IP address to a unique global IP address.
- **Server**: With this type you can specify inside servers of different services behind the NAT to be accessible to the outside world. Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

Table 27 summarizes these types.

Table 27 NAT mapping type

Type	IP Mapping	SMT Abbreviations
One-to-One	ILA1← → IGA1	1-1
Many-to-One (SUA/PAT)	ILA1← → IGA1 ILA2← → IGA1 …	M-1
Many-to-Many Overload	ILA1← → IGA1 ILA2← → IGA2 ILA3← → IGA1 ILA4← → IGA2 …	M-M Ov
Many-One-to-One	ILA1← → IGA1 ILA2← → IGA2 ILA3← → IGA3 …	M-1-1
Server	Server 1 IP← → IGA1 Server 2 IP← → IGA1 Server 3 IP← → IGA1	Server

Using NAT

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Business Secure Router.

SUA (Single User Account) versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Business Secure Router also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You can enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example, both FTP and web service), it is better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

With many residential broadband ISP accounts you cannot run any server processes (such as a Web or FTP server) from your location. Your ISP periodically checks for servers and can suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default server IP address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a Default Server IP Address, the Business Secure Router discards all packets received for ports that are not specified here or in the remote management setup.

Port forwarding: Services and Port Numbers

The most often used port numbers are shown in Table 28. Refer to *Assigned Numbers* (RFC 1700) for further information about port numbers. Refer to the Supporting CD for more examples and details on SUA/NAT.

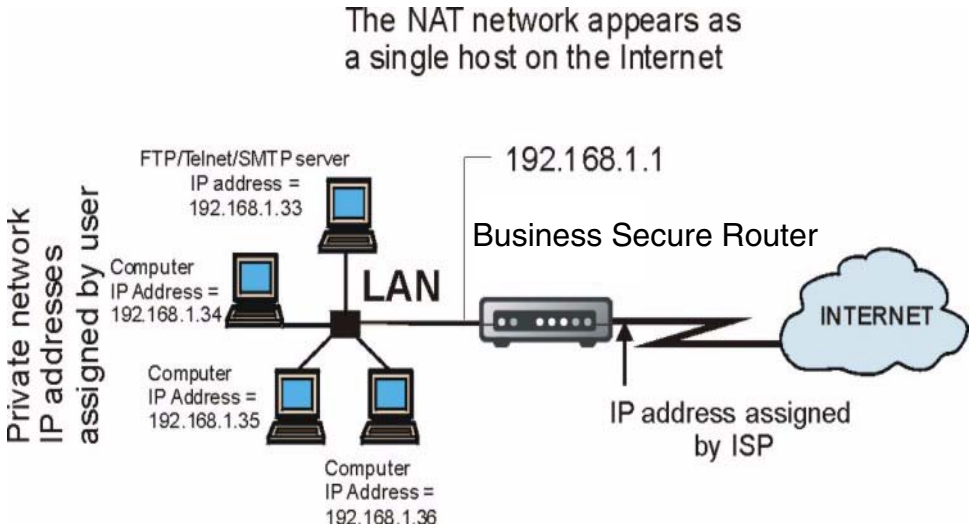
Table 28 Services and port numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Configuring servers behind SUA (example)

For example, you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35, as shown in Figure 37.

Figure 37 Multiple servers behind NAT example



Configuring SUA Server

Note: If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen are discarded.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to Chapter 10, “Firewalls,” on page 155 and Chapter 11, “Firewall screens,” on page 171 for port numbers commonly used for particular services.

Figure 38 SUA/NAT setup

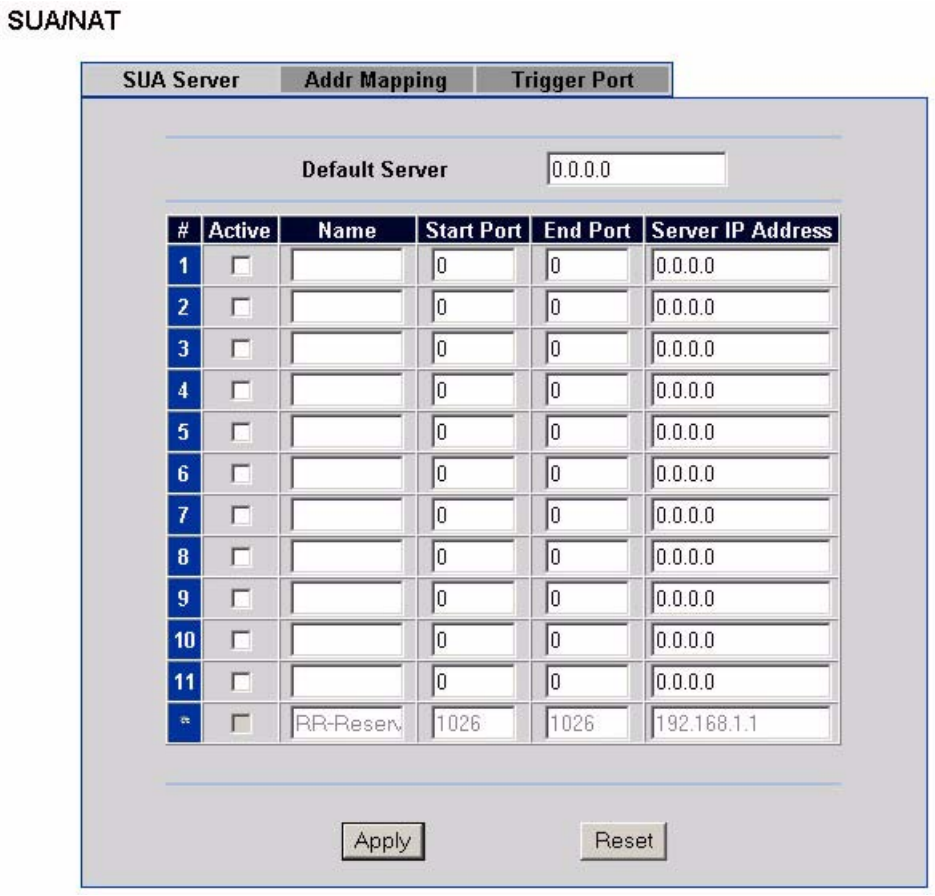


Table 29 describes the fields in Figure 38.

Table 29 SUA/NAT setup

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen are discarded.
#	Number of an individual SUA server entry.

Table 29 SUA/NAT setup

Label	Description
Active	Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to clear your changes.

Configuring Address Mapping

Ordering your rules is important because the Business Secure Router applies the rules in the order that you specify. When a rule matches the current packet, the Business Secure Router takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule is pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and you configure rule number 9. In the set summary screen, the new rule becomes rule 7, not 9. If you delete rule 4, rules 5 to 7 are pushed up by 1 rule, so old rules 5, 6, and 7 become new rules 4, 5, and 6.

To change your Business Secure Router's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown in Figure 39.

Figure 39 Address Mapping

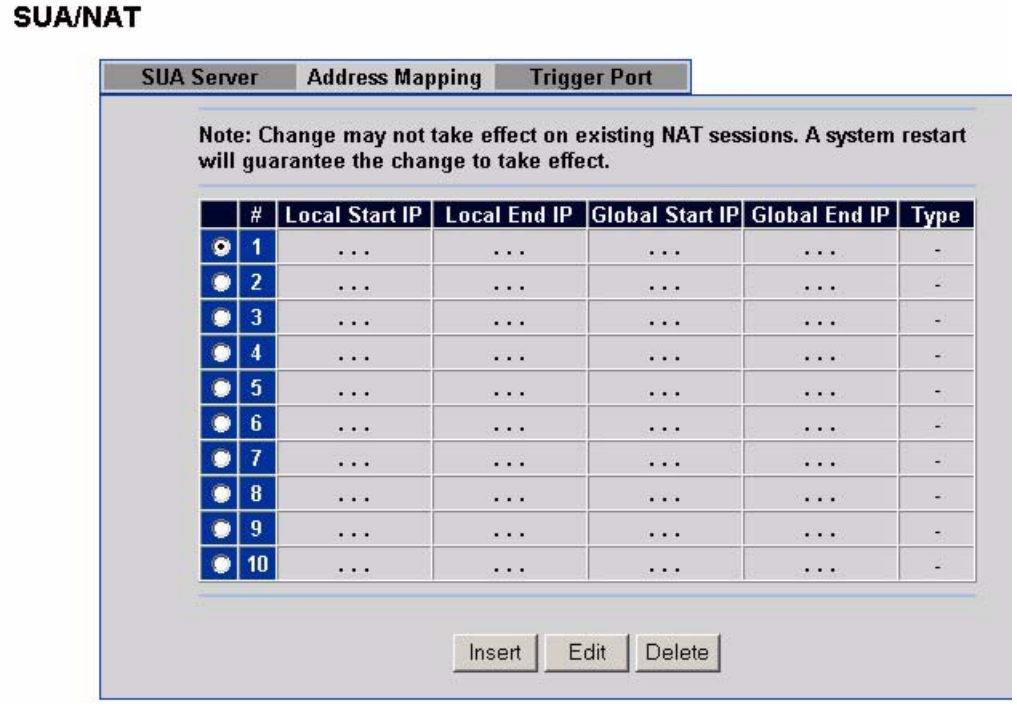

SUA/NAT
SUA Server
Address Mapping
Trigger Port
Note: Change may not take effect on existing NAT sessions. A system restart will guarantee the change to take effect.
Local Start IP Local End IP Global Start IP Global End IP Type
1 2 3 4 5 6 7 8 9 10
Insert
Edit
Delete

Table 30 describes the fields in Figure 39.

Table 30 Address Mapping

Label	Description
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 30 Address Mapping

Label	Description
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), the Single User Account feature. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** permits you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Edit	Click **Edit** to go to the **Address Mapping Rule** screen.
Delete	Click **Delete** to delete an address mapping rule.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown in Figure 40.

Figure 40 Address Mapping edit

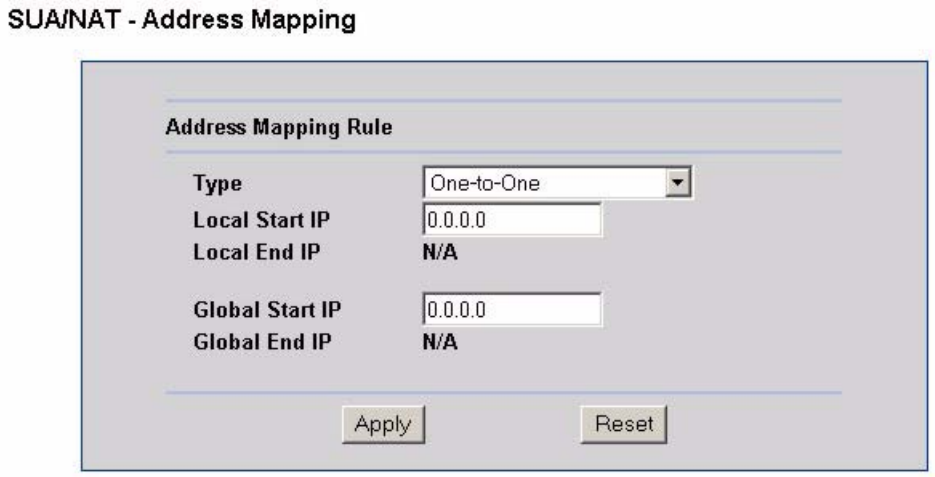


Table 31 describes the fields in Figure 40.

Table 31 Address Mapping edit

Label	Description
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: With this type, you can specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.

Table 31 Address Mapping edit

Label	Description
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Trigger Port Forwarding

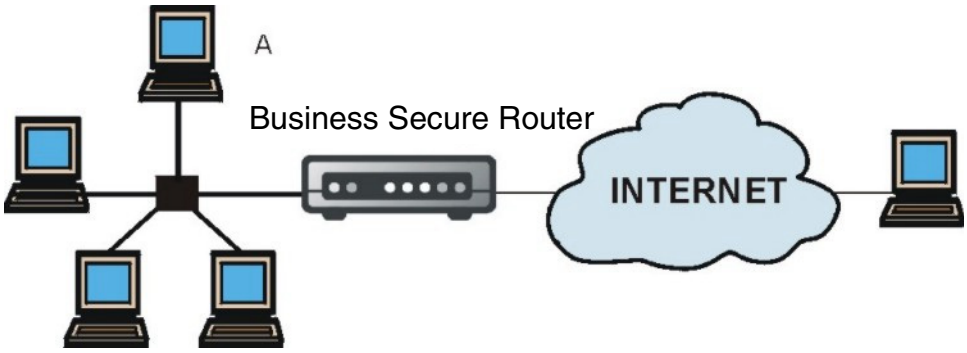
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Business Secure Router records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a trigger port). When the WAN port on the Business Secure Router receives a response with a specific port number and protocol (incoming port), the Business Secure Router forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way, you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Trigger Port Forwarding example

Figure 41 illustrates an example of trigger port forwarding.

Figure 41 Trigger Port Forwarding process: example



1. Jane (A) requests a file from the Real Audio server (port 7070).
2. Port 7070 is a trigger port and causes the Business Secure Router to record Jane's computer IP address. The Business Secure Router associates Jane's computer IP address with the incoming port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The Business Secure Router forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The Business Secure Router times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Two points to remember about Trigger Ports

Trigger events only happen on data that is coming from inside the Business Secure Router and going to the outside.

If an application needs a continuous data stream, that port (range) is tied up so that another computer on the LAN cannot trigger it.

Configuring Trigger Port Forwarding

To change trigger port settings of your Business Secure Router, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown in Figure 42.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 42 Trigger Port

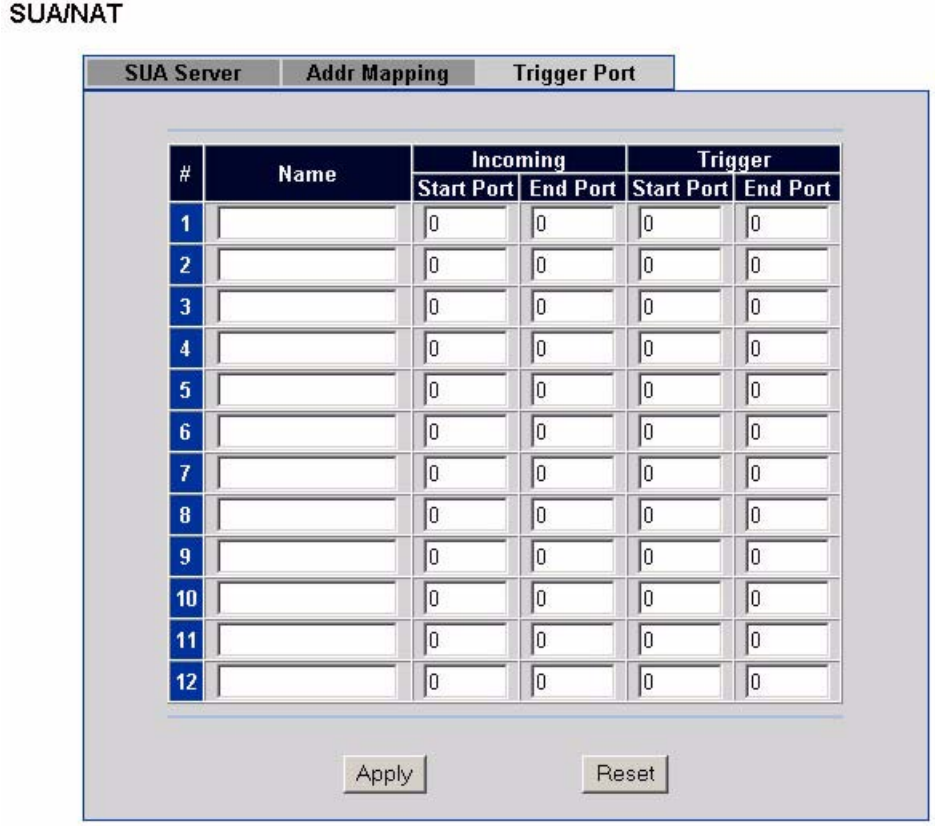


Table 32 describes the fields in Figure 42.

Table 32 Trigger Port

Label	Description
No.	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted, including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Business Secure Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Business Secure Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

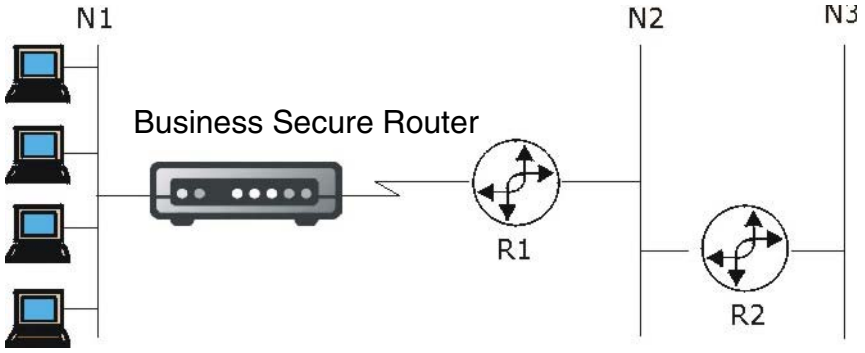
Chapter 9
Static Route screens

This chapter shows you how to configure static routes for your Business Secure Router.

Static Route overview

Each remote node specifies only the network to which the gateway is directly connected, and the Business Secure Router has no knowledge of the networks beyond. For instance, the Business Secure Router knows about network N2 in Figure 43 through remote node Router 1. However, the Business Secure Router is unable to route a packet to network N3 because it does not know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the Business Secure Router about the networks beyond the remote nodes.

Figure 43 Example of Static Routing topology



Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.

Note: The first static route entry is for the default WAN route. You cannot modify or delete this static default route.

Figure 44 Static Route screen

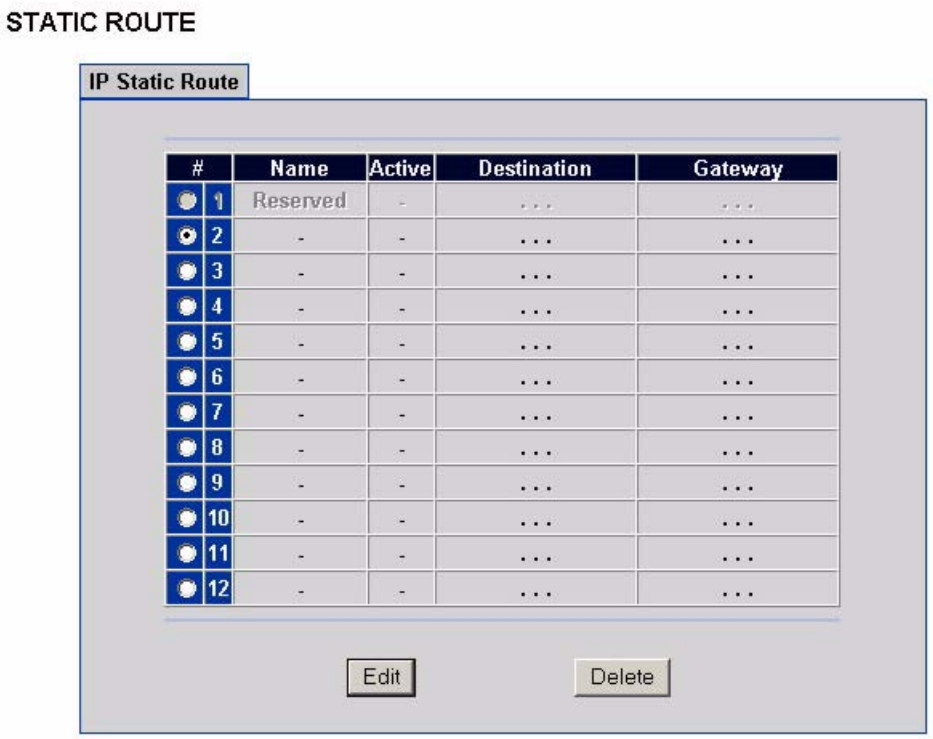


Table 33 describes the fields in Figure 43.

Table 33 IP Static Route summary

Label	Description
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the Business Secure Router's LAN or WAN port. The gateway helps forward packets to their destinations.
Edit	Click a static route index number and then click **Edit** to set up a static route on the Business Secure Router.

Configuring Route entry

Select a static route index number and click **Edit**. The screen is illustrated in Figure 45. Fill in the required information for each static route.

Figure 45 Edit IP Static Route

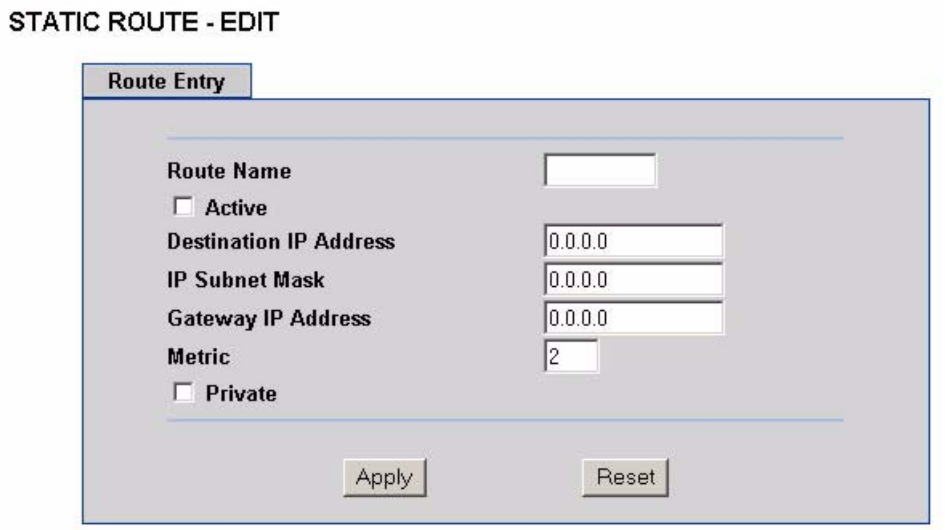


Table 34 describes the fields in Figure 45.

Table 34 Edit IP Static Route

Label	Description
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate or deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the Business Secure Router's LAN or WAN port. The gateway helps forward packets to their destinations.

Table 34 Edit IP Static Route

Label	Description
Metric	Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Business Secure Router includes this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 10
Firewalls

This chapter gives some background information on firewalls and introduces the Business Secure Router firewall.

Firewall overview

Originally, the term firewall referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access control policy between two networks. It can also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It must never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information security policy. In addition, specific policies must be implemented within the firewall itself.

Types of firewalls

There are three main types of firewalls:

1. Packet Filtering firewalls
2. Application level firewalls
3. Stateful Inspection firewalls

Packet Filtering firewalls

Packet filtering firewalls restrict access based on the source or destination computer network address of a packet and the type of application.

Application level firewalls

Application level firewalls restrict access by serving as proxies for external servers. Because they use programs written for specific Internet services, such as HTTP, FTP and Telnet, they can evaluate network packets for valid application specific data. Application level firewalls have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

1. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, because the application gateway is the only host whose name must be made known to outside systems.
2. Robust authentication and logging preauthenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

Stateful Inspection firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also inspect the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they often lack the granular application level access control or caching that some proxies support. For more information, see “Stateful inspection” on page 163.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

Introduction to the Business Secure Router firewall

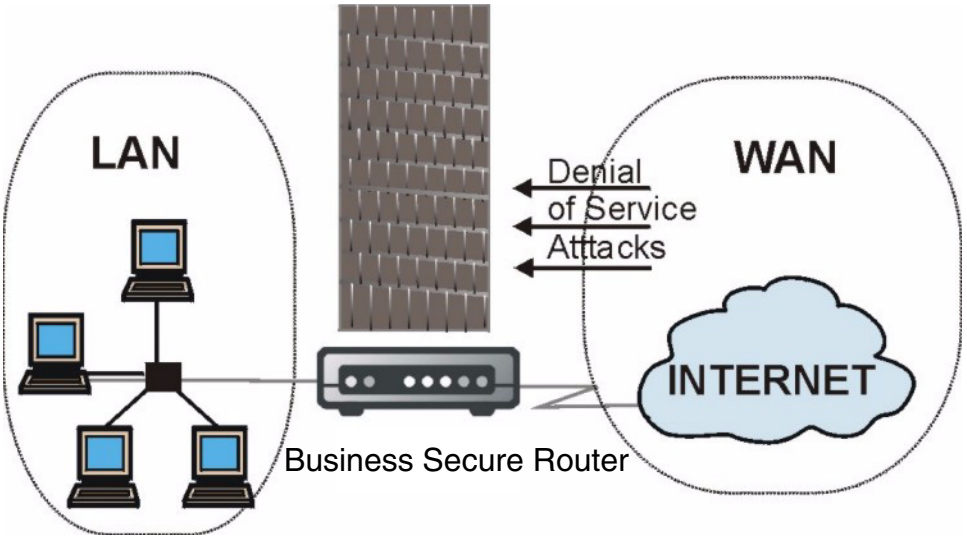
The Business Secure Router firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the WebGUI). The Business Secure Router's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Business Secure Router can be used to prevent theft, destruction and modification of data, as well as log events, which is important to the security of your network. The Business Secure Router also has packet filtering capabilities.

The Business Secure Router is installed between the LAN and a broadband modem connecting to the Internet, so that it can allow it to act as a secure gateway for all data passing between the Internet and the LAN.

The Business Secure Router has one Ethernet WAN port and four Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers have access to Internet services such as e-mail, FTP, and the World Wide Web. However, inbound access is not allowed unless the remote host is authorized to use a specific service.

Figure 46 Business Secure Router firewall application



Denial of Service

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Business Secure Router is preconfigured to automatically detect and thwart currently known DoS attacks.

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An extension number, called the TCP port or UDP port, identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol) and POP3 (E-mail). For example, Web traffic uses TCP port 80, by default.

When computers communicate on the Internet, they use the client/server model, where the server listens on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Note that, while a computer can be intended for use over a single port, such as Web on port 80, other ports are also active and vulnerable to attack by hackers.

Some of the most common IP ports are:

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Types of DoS attacks

There are four types of DoS attacks:

- Those that exploit bugs in a TCP/IP implementation.
- Those that exploit weaknesses in the TCP/IP specification.
- Brute force attacks that flood a network with useless data.
- IP Spoofing.

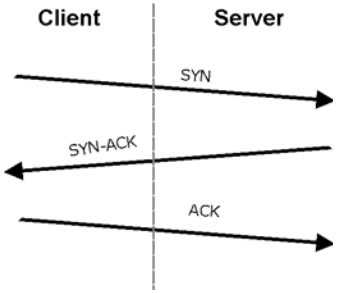
1 Ping of Death and Teardrop attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

Ping of Death uses a ping utility to create an IP packet that exceeds the maximum 65 536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system, and can cause systems to crash, hang, or reboot.

Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, “This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet.” The Teardrop program creates a series of IP fragments with overlapping offset fields. After these fragments are reassembled at the destination, some systems crash, hang, or reboot.

2 Weaknesses in the TCP/IP specification leave it open to SYN Flood and LAND attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

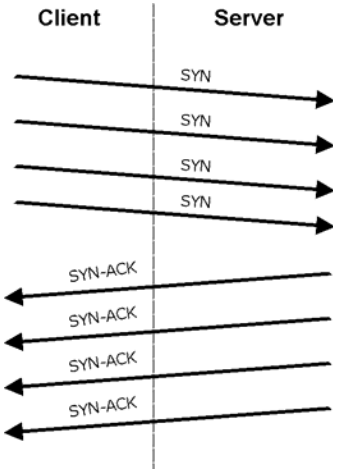
Figure 47 Three-way handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

SYN Attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system ignores all incoming SYN requests, making the system unavailable for legitimate users.

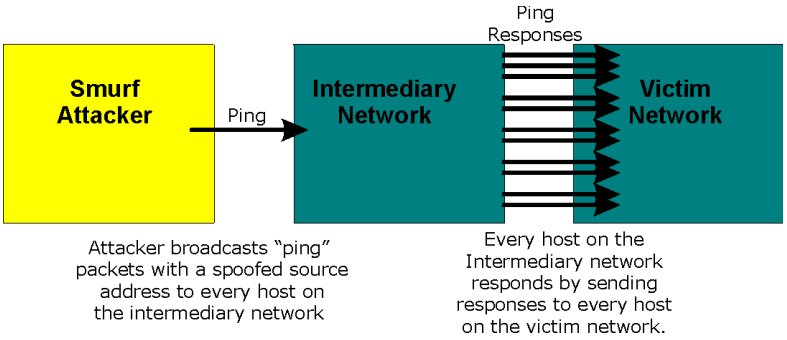
Figure 48 SYN flood



In a LAND Attack, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3 A brute force attack, such as a Smurf attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router broadcasts the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this creates a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic not only clogs up the intermediary network, but also congests the network of the spoofed source IP address, known as the victim network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 49 Smurf attack



- ICMP vulnerability

ICMP is an error reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 35 ICMP commands that trigger alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are shown in Table 36— all others are illegal.

Table 36 Legal NetBIOS commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in Table 37.

Table 37 Legal SMTP commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes, when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall and gain knowledge of the network topology inside the firewall.

4 Often, many DoS attacks also employ a technique known as IP Spoofing as part of their attack. IP Spoofing can be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and is allowed through the router or firewall. The Business Secure Router blocks all IP Spoofing attempts.

Stateful inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access an outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This remembering is called saving the state. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The Business Secure Router uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the Business Secure Router’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 50 Stateful inspection

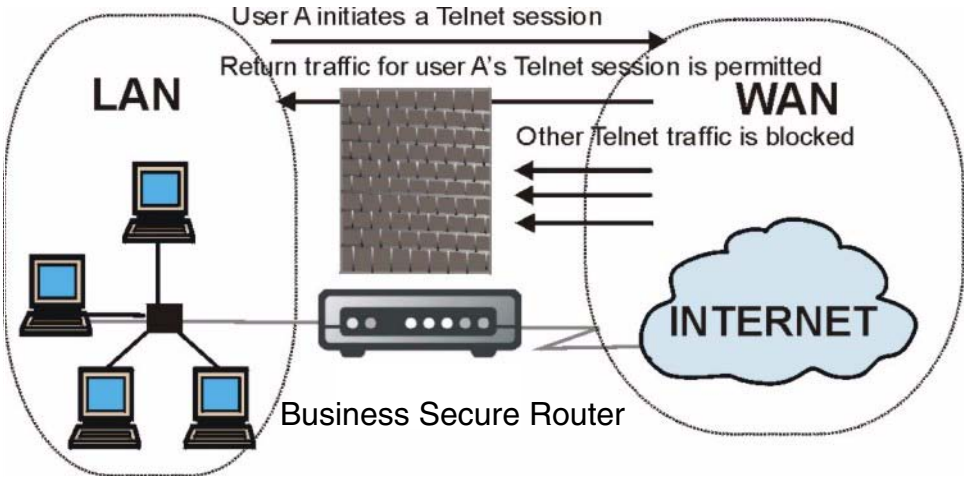


Figure 50 shows the Business Secure Router's default firewall rules in action, and demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However, other Telnet traffic initiated from the WAN is blocked.

Stateful inspection process

In the following example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet is dropped at this point).

3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, the **Action for packets that don't match firewall rules** field determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. You can modify the inbound extended access list temporary entries based on the updated state information, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

Stateful inspection and the Business Secure Router

Additional rules can be defined to extend or override the default rules. For example, a rule can be created that will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.

- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections can either be defined by the upper protocols (for instance, TCP), or by the Business Secure Router itself (as with the virtual connections created for UDP and ICMP).

TCP security

The Business Secure Router uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are initiation packets. All packets that do not have this flag structure are called subsequent packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, someone is trying to make a connection from the Internet into the LAN. Except in a few special cases, (see "Upper layer protocols" on page 167), these packets are dropped and logged.

If an initiation packet originates on the LAN, someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection is allowed. A cache entry is added, which includes connection information such as IP addresses, TCP ports, and sequence numbers.

After the Business Secure Router receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection that originated on the LAN).

UDP/ICMP security

UDP and ICMP do not contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build virtual connections in the cache.

For instance, any UDP packet that originates on the LAN creates a cache entry. Its IP address and port pairs are stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information are allowed back in through the firewall.

A similar situation exists for ICMP, except that the Business Secure Router is even more restrictive. Specifically, only outgoing echoes allow incoming echo replies, outgoing address mask requests allow incoming address mask replies, and outgoing timestamp requests allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they can be used to reroute traffic through attacking machines.

Upper layer protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a control connection, which is used for sending commands between endpoints, and then data connections, which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server opens a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet is normally rejected.

In order to achieve the above scenario, the Business Secure Router inspects the application level FTP data. Specifically, it searches for outgoing PORT commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the WebGUI's Custom Ports feature to do this.

Guidelines for enhancing security with your firewall

1. Change the default password via SMT or WebGUI.
2. Think about access control before you connect your device to the network in any way. Access to the console port can give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can Telnet into your router.
4. Do not enable any local service (such as SNMP or NTP) that you do not use. Any enabled service can present a potential security risk. A determined hacker can find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

Packet filtering vs. firewall

Below are some comparisons between the filtering and firewall functions of the Business Secure Router.

Packet filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When to use filtering

1. To block or allow LAN packets by their MAC addresses.
2. To block or allow special IP packets that are neither TCP nor UDP, nor ICMP packets.
3. To block or allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host or network A and outside host or network B. If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block or allow IP trace route.

Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of the connections it handles, so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.

- The firewall uses session filtering, or smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When to use the firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule, making the firewall a better choice when complex rules are required.
3. To selectively block or allow inbound or outbound traffic between inside host or networks and outside host or networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block any specific URL traffic that occurs in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 11
Firewall screens

This chapter shows you how to configure your Business Secure Router firewall.

Access methods

The WebGUI is, by far, the most comprehensive firewall configuration tool your Business Secure Router has to offer. For this reason, Nortel recommends that you configure your firewall using the WebGUI. With SMT screens, you can activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, refer to *Nortel Business Secure Router 222 Configuration — Advanced* (NN47922-501) for firewall CLI commands.

Firewall policies overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

LAN to LAN/Business Secure Router	WAN to LAN
LAN to WAN	WAN to WAN/Business Secure Router

By default, Business Secure Router's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/Business Secure Router
  This allows computers on the LAN to manage the Business Secure Router and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN

By default, the Business Secure Router's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/Business Secure Router
  This prevents computers on the WAN from using the Business Secure Router as a gateway to communicate with other computers on the WAN, or to manage the Business Secure Router, or both.

You can define additional rules and sets or modify existing ones, but exercise extreme caution in doing so.

Note: If you configure firewall rules without a good understanding of how they work, you can inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you can create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Business Secure Router's default rules.

Rule logic overview

Note: Study these points carefully before configuring rules.

Rule checklist

1. State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to?
4. What IP services are affected?
5. What computers on the LAN are affected (if any)?
6. What computers on the Internet are affected? The more specific, the better. For example, if traffic is allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Security ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, a rule that blocks just certain users can be more effective.
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users can connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the WebGUI screens.

Key fields for configuring rules

Action

Set the action to either **Block** or **Forward**.

Note: Block means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. For more information on predefined services, see "Predefined services" on page 188.

Source address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs, or a subnet?

Destination address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Connection direction examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/Business Secure Router rules apply to packets coming in through the LAN interface that are destined for either the Business Secure Router's LAN interface itself or a different subnet on the LAN. A management session through

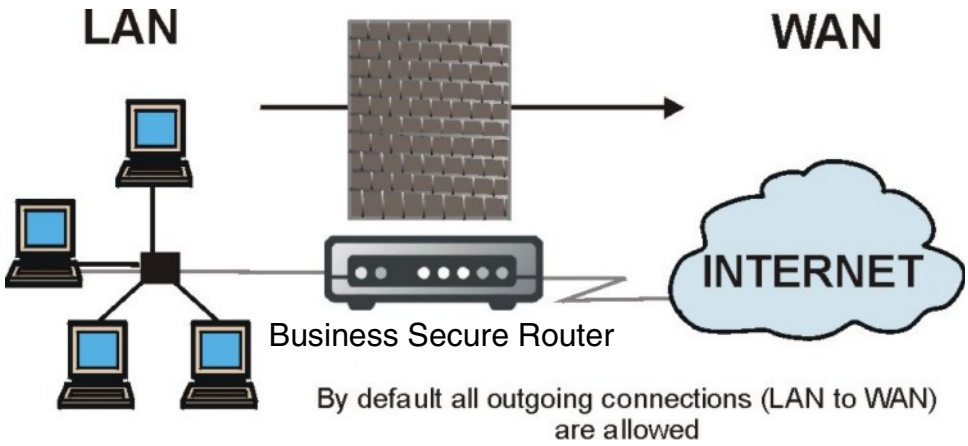
the LAN interface is an example of traffic destined for the Business Secure Router's LAN interface itself. You can also use LAN to LAN/Business Secure Router rules with IP alias to control routing between two subnets on the LAN.

WAN to WAN/Business Secure Router rules apply to packets coming in through the WAN interface that are destined for either the Business Secure Router's WAN interface itself or a different subnet on the WAN. A management session through the WAN interface is an example of traffic destined for the Business Secure Router's WAN interface itself. By default, the Business Secure Router stops WAN computers from using the Business Secure Router as a gateway to communicate with other computers on the WAN. You can configure one of these rules to allow a WAN computer to manage the Business Secure Router.

LAN to WAN rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed unrestricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN.

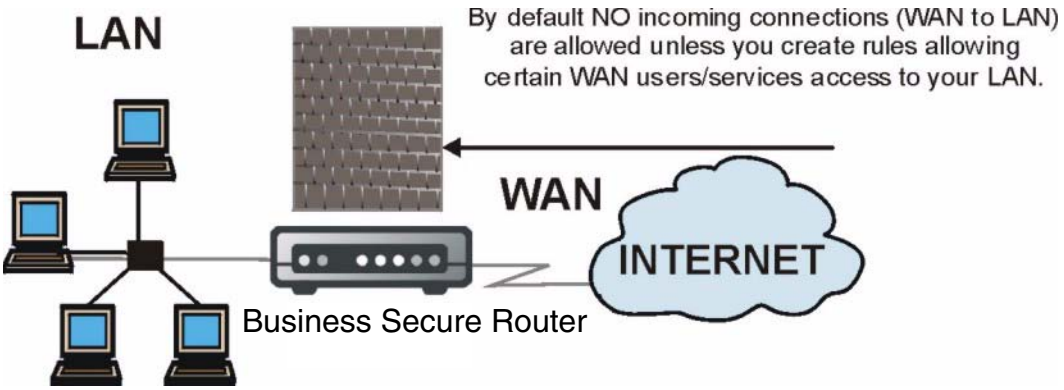
Figure 51 LAN to WAN traffic



WAN to LAN rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you want to allow certain WAN users to have access to your LAN, you need to create custom rules to allow it.

Figure 52 WAN to LAN traffic


LAN
By default NO incoming connections (WAN to LAN)
are allowed unless you create rules allowing
certain WAN users/services access to your LAN.
WAN
INTERNET
Business Secure Router

Configuring firewall

Click **FIREWALL** to open the **Summary** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in Figure 53.

The Business Secure Router applies the firewall rules in order, starting from the first rule for a packet's direction of travel. When the traffic matches a rule, the Business Secure Router takes the action in the rule and stops checking the firewall rules.

For example, you have one general rule that blocks all LAN to WAN IRC (Internet Relay Chat). And you have another rule that allows IRC traffic from your company president's LAN IP address to go to the WAN. In order for the president's IRC traffic to get through, the rule for the president's IP address must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic comes first, all LAN to WAN IRC traffic matches that rule and the Business Secure Router drops the president's connection and does not check any other firewall rules.

If you list a general rule before a specific rule, traffic that you want to be controlled by the specific rule can get the general rule applied to it instead. Any traffic that does not match the first firewall rule matches the default rule and the Business Secure Router forwards the traffic.

Note: If an alternate gateway on the LAN has an IP address in the same subnet as the Business Secure Router's LAN IP address, return traffic does not go through the Business Secure Router. This is called an asymmetrical or triangle route, and causes the Business Secure Router to reset the connection, as the connection has not been acknowledged.
Note: Allowing asymmetrical routes can let traffic from the WAN go directly to the LAN without passing through the Business Secure Router. A better solution is to use IP alias to put the Business Secure Router and the backup gateway on separate subnets. See the Appendix B "Triangle Route" of *Nortel Business Secure Router 222 Configuration — Advanced* (NN47922-501) for more about triangle route topology.

Figure 53 Enabling the firewall

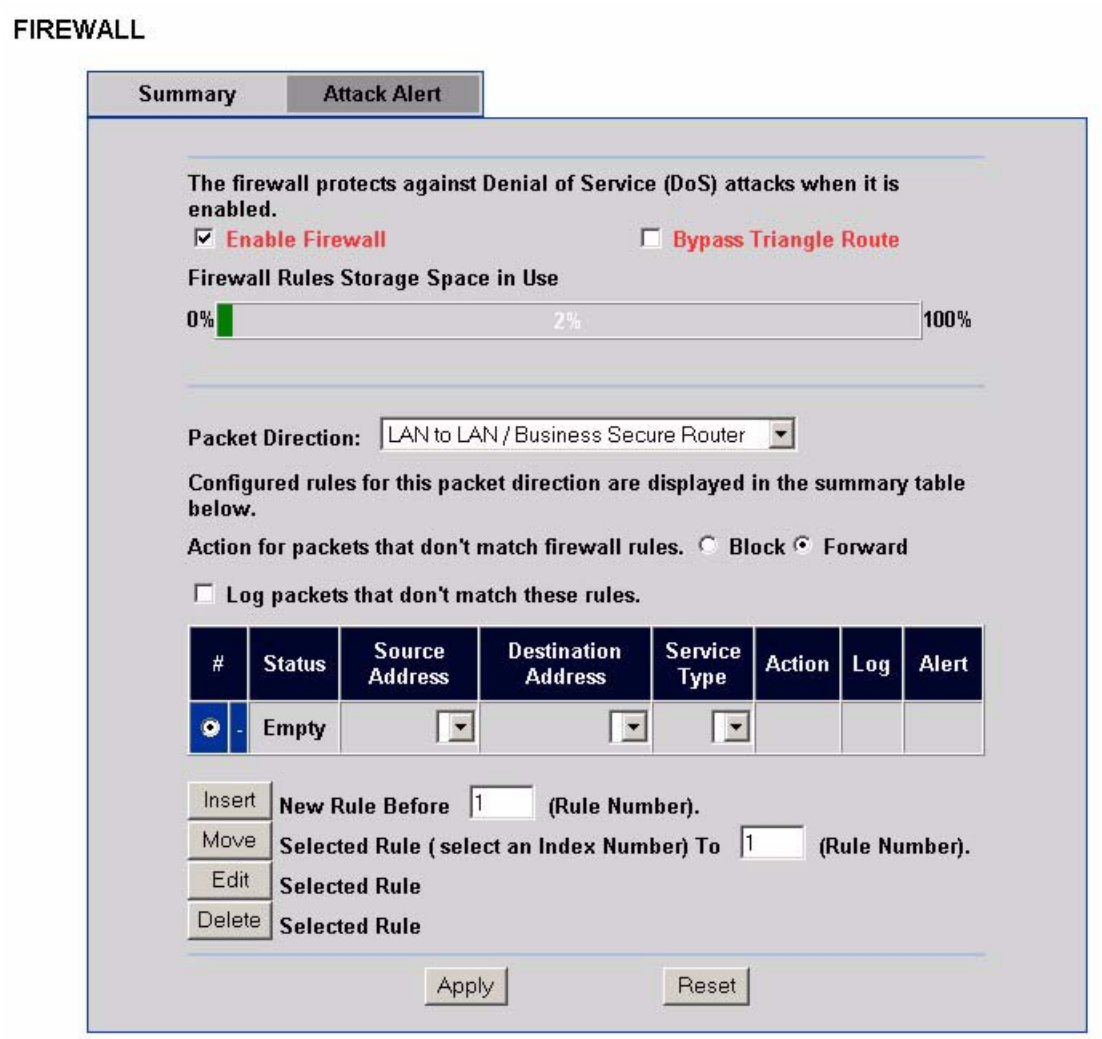


Table 38 describes the fields in Figure 53.

Table 38 Firewall rules summary: First screen

Label	Description
Enable Firewall	Select this check box to activate the firewall. The Business Secure Router performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. The firewall allows traffic to go through your VPN tunnels.

Table 38 Firewall rules summary: First screen

Label	Description
Bypass Triangle Route	Select this check box to have the Business Secure Router permit the use of asymmetrical route topology on the network (not reset the connection).
Firewall Rules Storage Space in Use	This read-only bar shows how much of the Business Secure Router's memory for recording firewall rules is currently being used. The bar turns from green to red when the maximum is approached. You can typically configure up to ten rules per traffic direction.
Packet Direction	Use the drop-down list to select a direction of travel of packets for which you want to display firewall rules.
Block/ Forward	Use the option buttons to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log packets that don't match these rules.	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field allows you to reorder your rules.
Status	This field displays whether a firewall is turned on (**Active**) or not (**Inactive**). Rules that have not been configured display **Empty**.
Source Address	This drop-down list displays the source addresses or ranges of addresses to which this firewall rule applies. Note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list displays the destination addresses or ranges of addresses to which this firewall rule applies. Note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list displays the services to which this firewall rule applies. Note that a blank service type is equivalent to **Any**. For more information, see Table 42 on page 189.
Action	This is the specified action for the selected rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**), or no log is created (**None**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.

Table 38 Firewall rules summary: First screen

Label	Description
Insert	Type the index number for where you want to put a rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click **Insert** to display the screen where you configure a firewall rule.
Move	Select a rule’s Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Edit	Click **Edit** to create or edit a rule.
Delete	Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring firewall rules

Follow these directions to create a new rule.

In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type 1, your new rule becomes number 1 and the previous rule 1 (if there is one) becomes rule 2.

Click **Insert** to display the screen shown in Figure 54.

Figure 54 Creating and editing a firewall rule

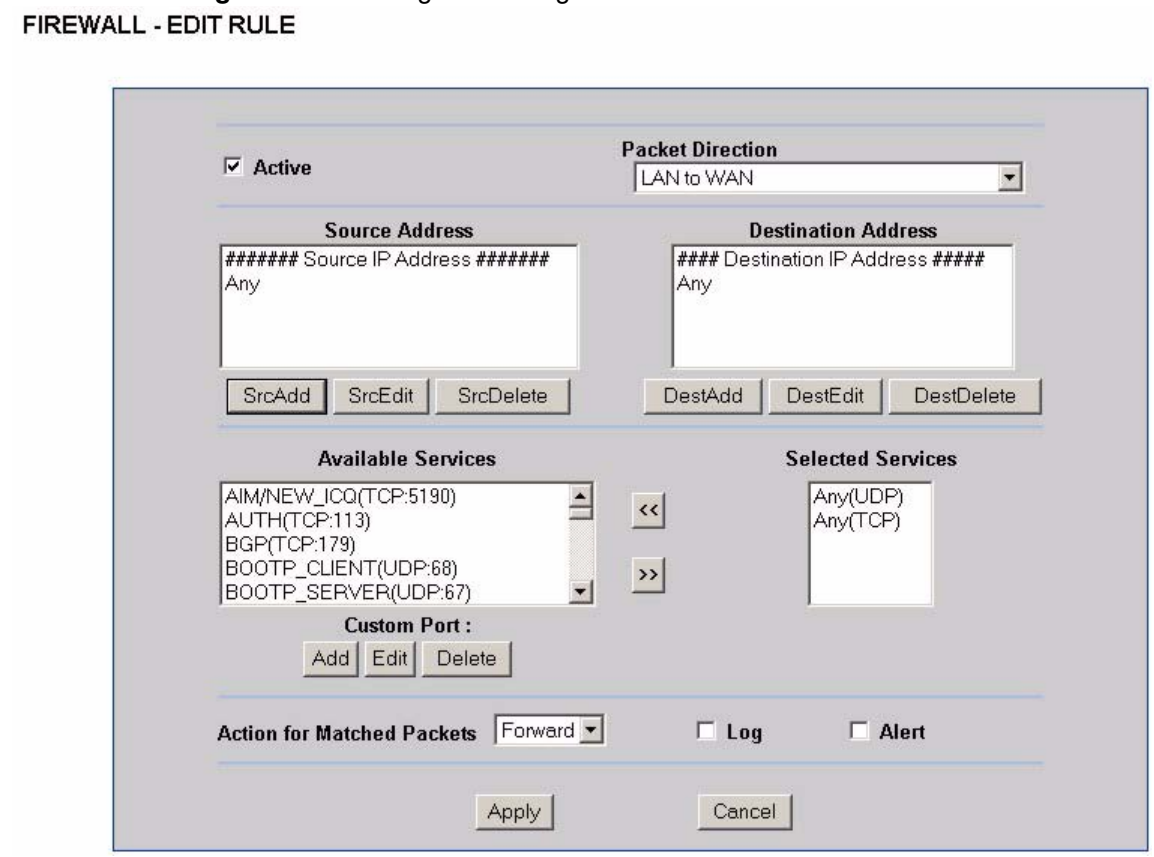


Table 39 describes the fields in Figure 54.

Table 39 Creating and editing a firewall rule

Label	Description
Active	Check the **Active** check box to have the Business Secure Router use this rule. Leave it unchecked if you do not want the Business Secure Router to use the rule after you apply it.
Packet Direction	Use the drop-down list to select the direction of packet travel to which you want to apply this firewall rule.

Table 39 Creating and editing a firewall rule

Label	Description
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. The source address can be a particular (single) IP, a range of IP addresses (for example, 192.168.1.10 to 192.169.1.50), a subnet or any IP address. See the next section for more information about adding and editing source addresses.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. The destination address can be a particular (single) IP, a range of IP addresses (for example, 192.168.1.10 to 192.169.1.50), a subnet or any IP address. See section “Configuring source and destination addresses” on page 183 for information about adding and editing destination addresses.
Services Available/ Selected Services	For more information on services available, see Table 42 on page 189. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an “*”) from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an “*”) from the **Available Services** list and click this button to remove the service.
Action for Matched Packets	Use the drop-down list to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the Business Secure Router record these logs.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Apply	Click **Apply** to save your changes to the Business Secure Router and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

Configuring source and destination addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the screen shown in Figure 55.

Figure 55 Adding or editing source and destination addresses

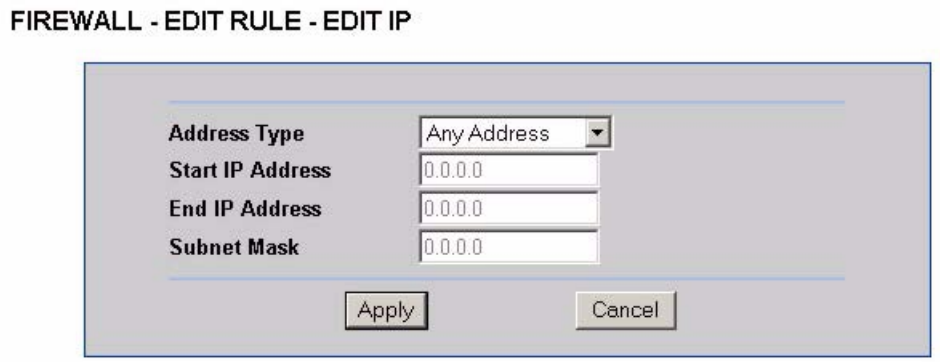


Table 40 describes the fields in Figure 55.

Table 40 Adding or editing source and destination addresses

Label	Description
Address Type	Select an option from the drop-down list that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here. Use a numerical IP address in dotted decimal notation (for example, 192.168.1.10).
End IP Address	Enter the ending IP address in a range here. Use a numerical IP address in dotted decimal notation (for example, 192.168.1.10).
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click **Apply** to save your changes to the Business Secure Router and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

Configuring custom ports

You can also configure customized ports for services not predefined by the *Business Secure Router* (see "Predefined services" on page 188 for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) Web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the screen illustrated in Figure 56.

Figure 56 Creating or editing a custom port

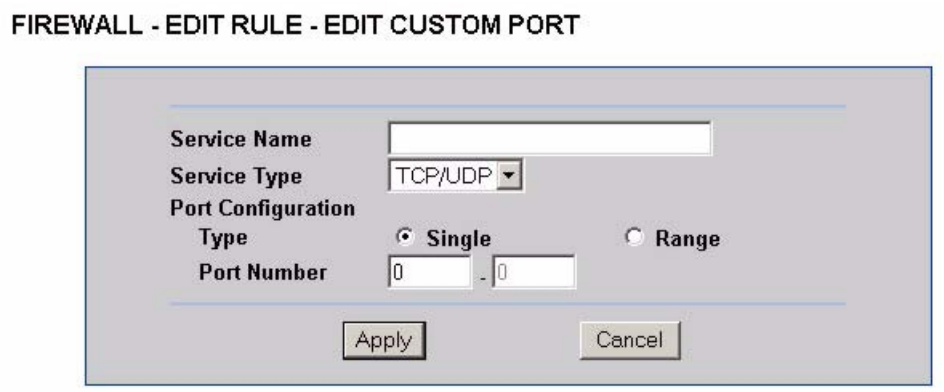


Table 41 describes the fields in Figure 56.

Table 41 Creating/Editing A Custom Port

Label	Description
Service Name	Enter a unique name to identify the service (a service that is not predefined in the Business Secure Router).
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop-down list.
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your changes to the Business Secure Router and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

Example firewall rule

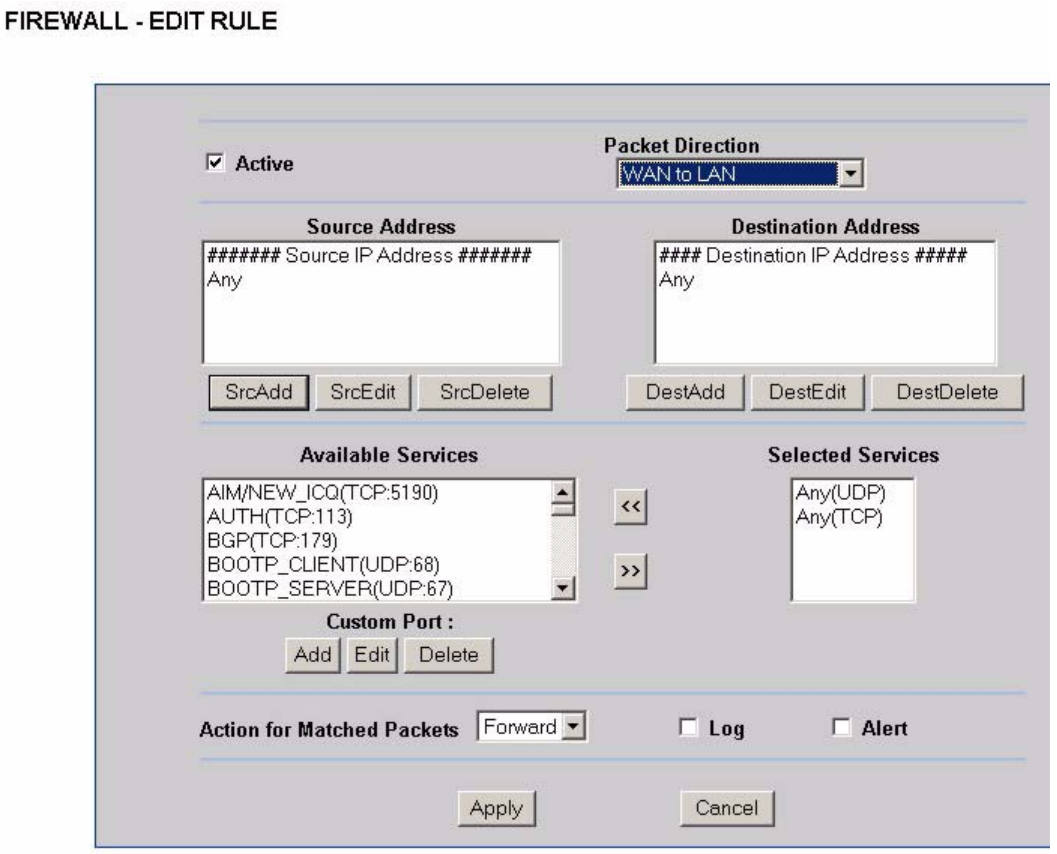
The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

1 Click the **Firewall** link and then the **Summary** tab.

2 In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

3 Click **Insert** to display the firewall rule configuration screen.

Figure 57 Firewall edit rule screen example

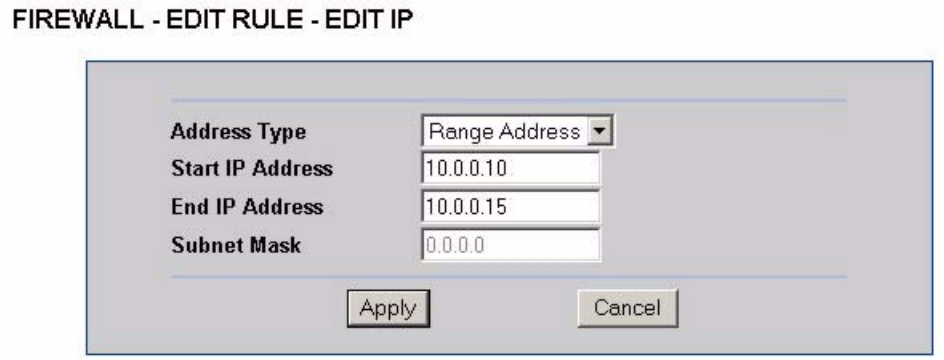


4 Select **WAN to LAN** as the **Packet Direction**.

5 Select **Any** in the **Destination Address** box and then click **DestEdit**.

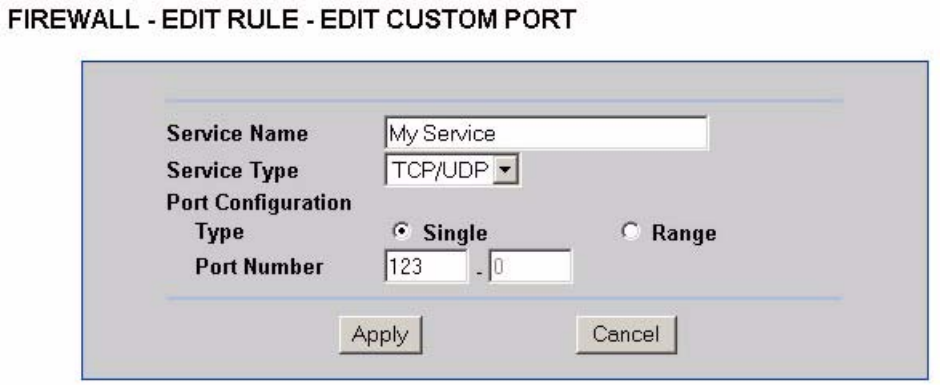
6 Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

Figure 58 Firewall rule edit IP example



7 In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as shown in Figure 59 and click **Apply**.

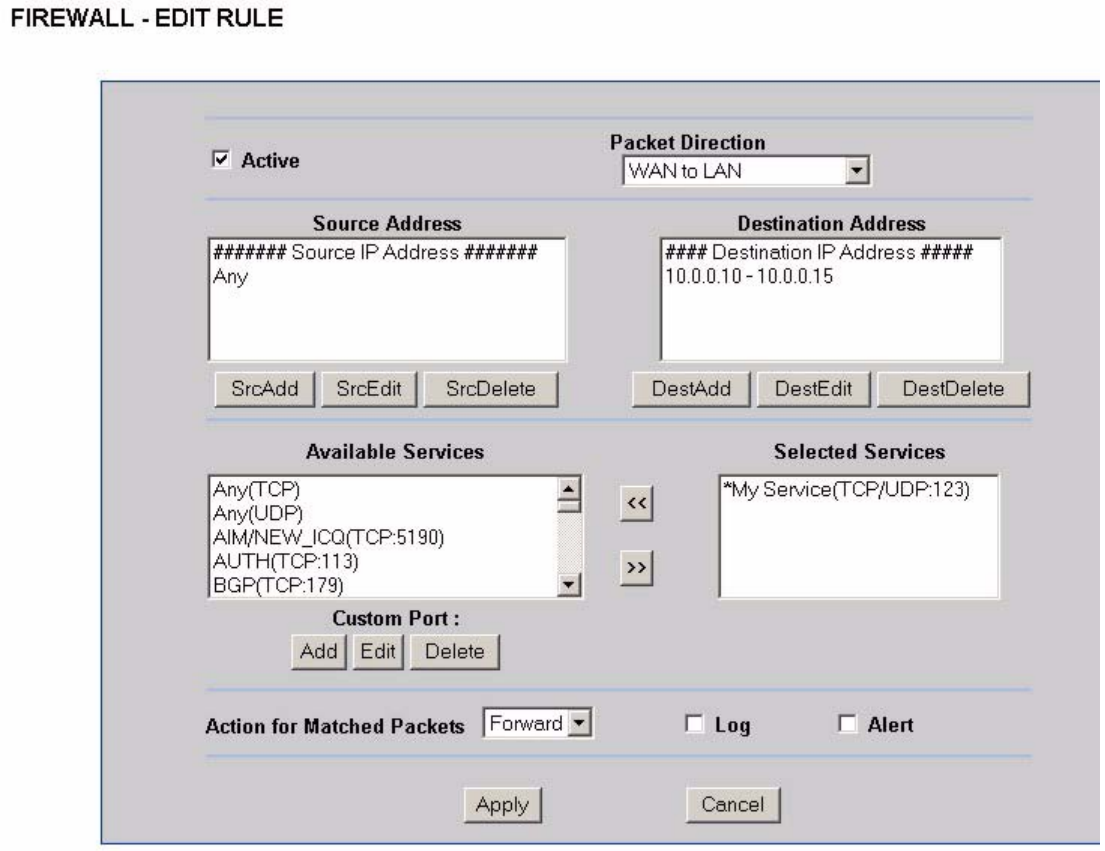
Figure 59 Edit custom port example



8 The firewall rule configuration screen displays. Use the arrows between **Available Services** and **Selected Services** to configure it as shown in Figure 60. Click **Apply** after you are done.

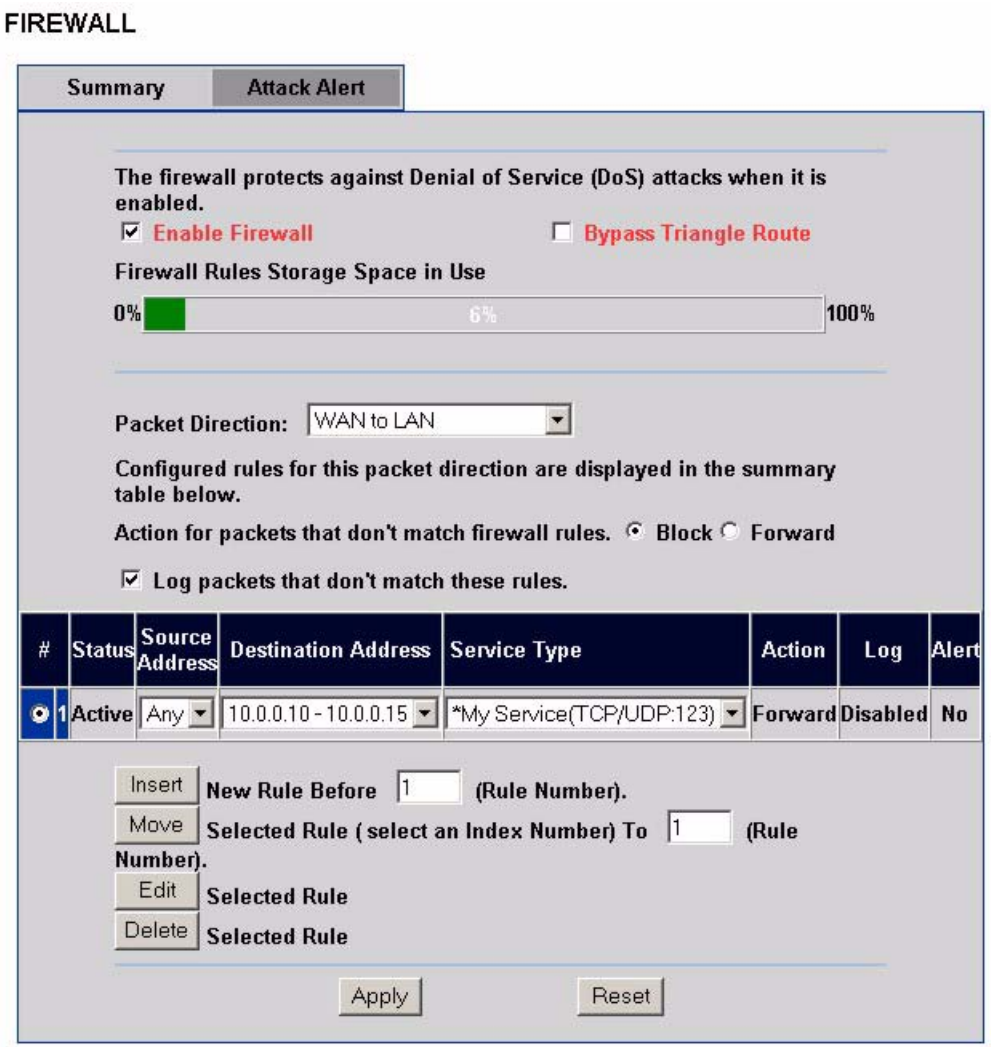
Note: Custom ports show up with an * before their names in the Services list box and the Rule Summary list box. Click **Apply** after you have created your custom port.

Figure 60 MyService rule configuration example



After completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen will look like the on illustrated in Figure 61. Rule 1: Allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN. Remember to click **Apply** after you finish configuring your rules to save your settings to the Business Secure Router.

Figure 61 My Service example rule summary



Predefined services

The **Available Services** list box in the **Edit Rule** screen (see Figure 54) displays all predefined services that the Business Secure Router already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there can be more than one IP protocol

type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services can also be configured using the **Custom Ports** function, which is discussed in "Configuring custom ports" on page 184.

Table 42 Predefined services

Service	Description
AIM/New-ICQ(TCP:5190)	AOL Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches Web names (for example, www.nortel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet-related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program is a program to enable fast transfer of files, including large files that cannot be sent by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol is a client/server protocol for the World Wide Web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.

Table 42 Predefined services

Service	Description
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System (NFS) is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer receive e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Logon.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

Table 42 Predefined services

Service	Description
SIP-V2(UDP:5060)	The Session Initiation Protocol (SIP) is an application layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.
SSH(TCP/UDP:22)	Secure Shell Remote Logon Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Using syslog, you can send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the logon and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

Alerts

Alerts are reports on events, such as attacks, that you want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(*Figure 62, check the **Generate alert when attack detected** check box) or when a rule is matched in the **Rule Edit** screen (see Figure 54). Configure the **Log Settings** screen to have the Business Secure Router send an immediate e-mail message to you when an event generates an alert.

Configuring attack alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen (Figure 62) you can choose to generate an alert whenever an attack is detected. For DoS attacks, the Business Secure Router uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Threshold values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values work fine for normal, small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

- The maximum number of opened sessions
- The minimum capacity of server backlog in your LAN network
- The CPU power of servers in your LAN network
- Network bandwidth
- Type of traffic for certain servers

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values must be reduced.
You must make any changes to the threshold values before you continue configuring firewall rules.

Half-open sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) indicates that a Denial of Service attack is occurring. For TCP, half-open means that the session has not reached the established state, and the TCP three-way handshake has not yet been completed (see Figure 47). For UDP, half-open means that the firewall has detected no return traffic.

The Business Secure Router measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

After the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the Business Secure Router starts deleting half-open sessions as required to accommodate new connection requests. The Business Secure Router continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

After the rate of new connection attempts rises above a threshold (**one-minute high**), the Business Secure Router starts deleting half-open sessions to accommodate new connection requests as required. The Business Secure Router continues to delete half-open sessions, as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one minute sample period.

TCP maximum incomplete and blocking period

An unusually high number of half-open sessions with the same destination host address indicates that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the Business Secure Router starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Period** timeout is 0 (the default), the Business Secure Router deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host never exceeds the threshold.
- If the **Blocking Period** timeout is greater than 0, the Business Secure Router blocks all new connection requests to the host giving the server time to handle the present connections. The Business Secure Router continues to block all new connection requests until the **Blocking Period** expires.

The Business Secure Router also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the screen shown in Figure 62.

Figure 62 Attack alert

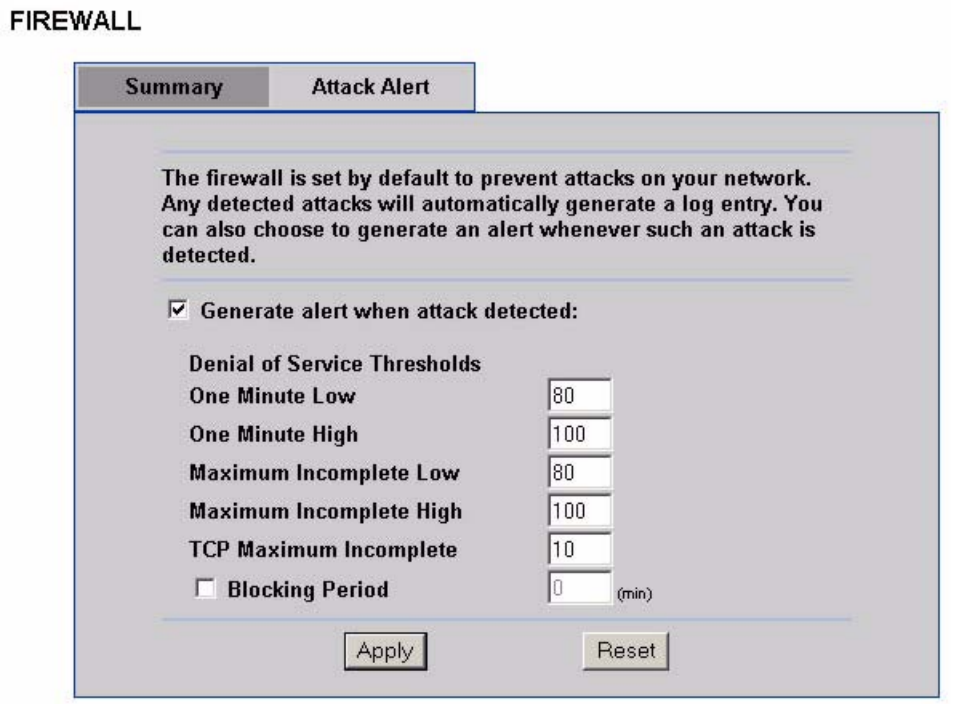


Table 43 describes the fields in Figure 62.

Table 43 Attack alert

Label	Description
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected.
Denial of Service Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Business Secure Router continues to delete half-open sessions, as necessary, until the rate of new connection attempts drops below this number.

Table 43 Attack alert

Label	Description
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Business Secure Router deletes half-open sessions, as required, to accommodate new connection attempts. The numbers, for example, 80 in the **One Minute Low** field and 100 in this field, cause the Business Secure Router to start deleting half-open sessions when more than 100 session establishment attempts are detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts are detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The Business Secure Router continues to delete half-open requests, as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Business Secure Router deletes half-open sessions, as required, to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. The above values, say 80 in the **Maximum Incomplete Low** field and 100 in this field, cause the Business Secure Router to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, choose a smaller number for a smaller network, a slower system or limited bandwidth.
Blocking Period	When **TCP Maximum Incomplete** is reached you can choose to either allow or block the next session. If you select the **Blocking Period** check box, any new sessions are blocked for the length of time you specify in the next field (min) and all old incomplete sessions are cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it gives the server some time to digest the loading.
(min)	Enter the length of **Blocking Period** in minutes.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 12
Content filtering

This chapter provides a brief overview of content filtering using the embedded WebGUI.

Introduction to content filtering

With Internet content filtering, you can create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and is not to be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Content Filter** to expand the Content Filter menus.

Restrict web features

The Business Secure Router can block web features such as ActiveX controls, Java applets, and cookies and disable web proxies.

Days and Times

With the Business Secure Router, you can also define time periods and days during which the Business Secure Router performs content filtering.

Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the screen show in Figure 63.

Figure 63 Content filter

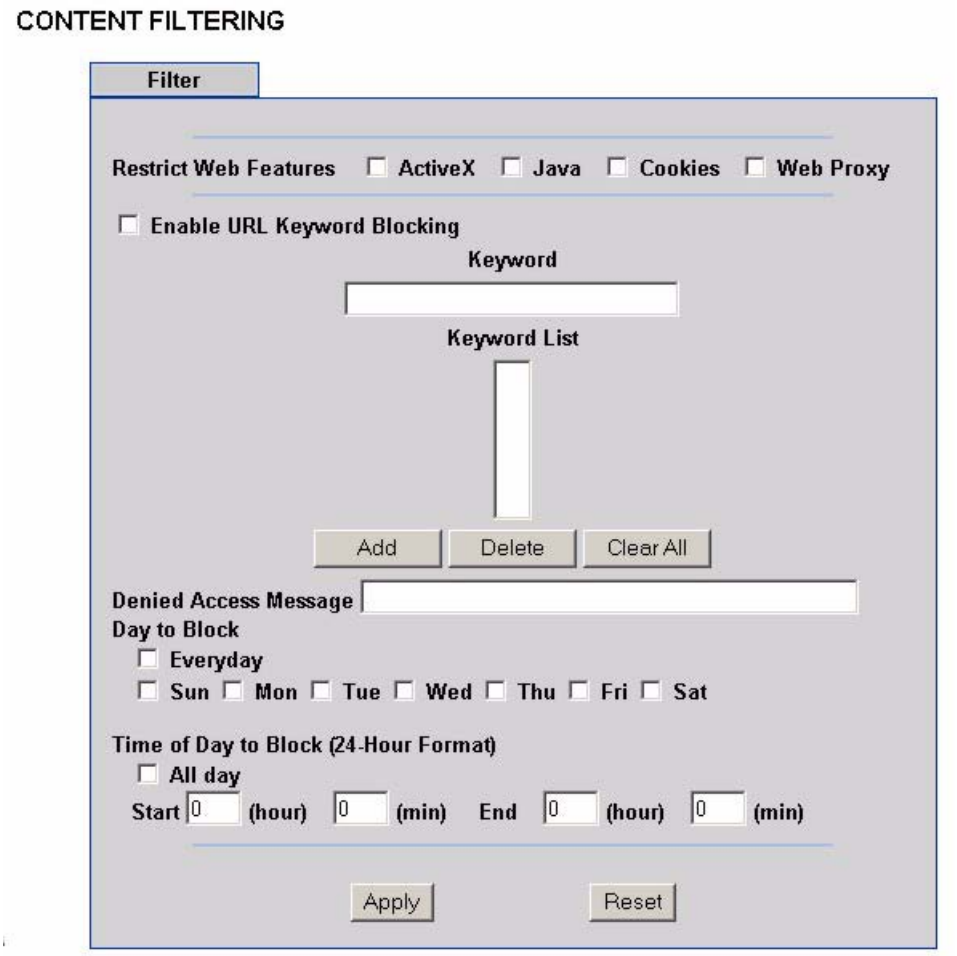


Table 44 describes the fields in Figure 63.

Table 44 Content filter

Label	Description
Restrict Web Features	Select the boxes to restrict a feature. When you download a page containing a restricted feature, that part of the web page appears blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The Business Secure Router can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword bad was enabled, all sites containing this keyword in the domain name or IP address will be blocked, for example, URL http://www.website.com/bad.html is blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You can use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will receive a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the Business Secure Router to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.

Table 44 Content filter

Label	Description
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the **All Day** check box to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

Chapter 13
VPN

This chapter introduces the basics of IPSec VPNs and covers the VPN WebGUI. See Chapter 20, “Logs Screens,” on page 371 for information about viewing logs and the appendices for IPSec log descriptions.

VPN

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control, and auditing technologies or services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

IPSec

Internet Protocol Security (IPSec) is a standards based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

Nortel Business Secure Router 222 VPN functions

You can use the Business Secure Router as either:

- A Contivity Client (for an encrypted connection to a single VPN router).

or

- As a VPN router that can have encrypted connections to multiple remote VPN routers. With this role, it can also serve as a termination point for encrypted connections from computers using Nortel's Contivity VPN Client 3.0, 5.01, 5.11, 6.01, 6.02, or 7.01 software.

See Table 1 on page 33 for details about the VPN specifications of the Nortel Business Secure Router 222.

VPN screens overview

Table 46 summarizes the main functions of the VPN screens.

Table 45 VPN Screens overview

Screens		Description
Summary		This screen lists all of your VPN rules.
	Contivity Client Rule Setup	Use these screens to configure simple VPN rules that have the Nortel Business Secure Router 222 operate as a VPN client.
	Branch Office Rule Setup	Use these screens to manually configure VPN rules that have the Nortel Business Secure Router 222 operate as a VPN router.
SA Monitor		Use this screen to display and manage active VPN connections.
Global Setting		Use this screen to configure the IPSec timer settings.
Client Termination		Use these screens to use the Nortel Business Secure Router 222 for encrypted connections from computers using Nortel's Contivity VPN Client software.

Security Association

A Security Association (SA) is a contract between two parties indicating which security parameters, such as keys and algorithms, they use.

Table 46 VPN Screens Overview

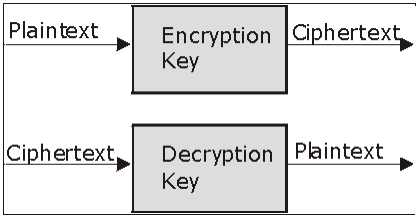
Screens		Description
Summary		This screen lists all of your VPN rules.
	Contivity Client Rule Setup	Use these screens to configure simple VPN rules that have the Nortel Business Secure Router 222 operate as a VPN client.
	Branch Office Rule Setup	Use these screens to manually configure VPN rules that have the Nortel Business Secure Router 222 operate as a VPN router.
SA Monitor		Use this screen to display and manage active VPN connections.
Global Setting		Use this screen to configure the IPSec timer settings.

Other terminology

Encryption

Encryption is a mathematical operation that transforms data from plaintext (readable) to ciphertext (scrambled text) using a key. The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption; it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 64 Encryption and decryption



Data confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

Data integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data is not altered during transmission.

Data origin authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

VPN applications

The Business Secure Router supports the following VPN applications:

- Linking Two or More Private Networks Together

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

  When NAT is enabled between the WAN and the LAN, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users can access all computers that use private IP addresses on the LAN.

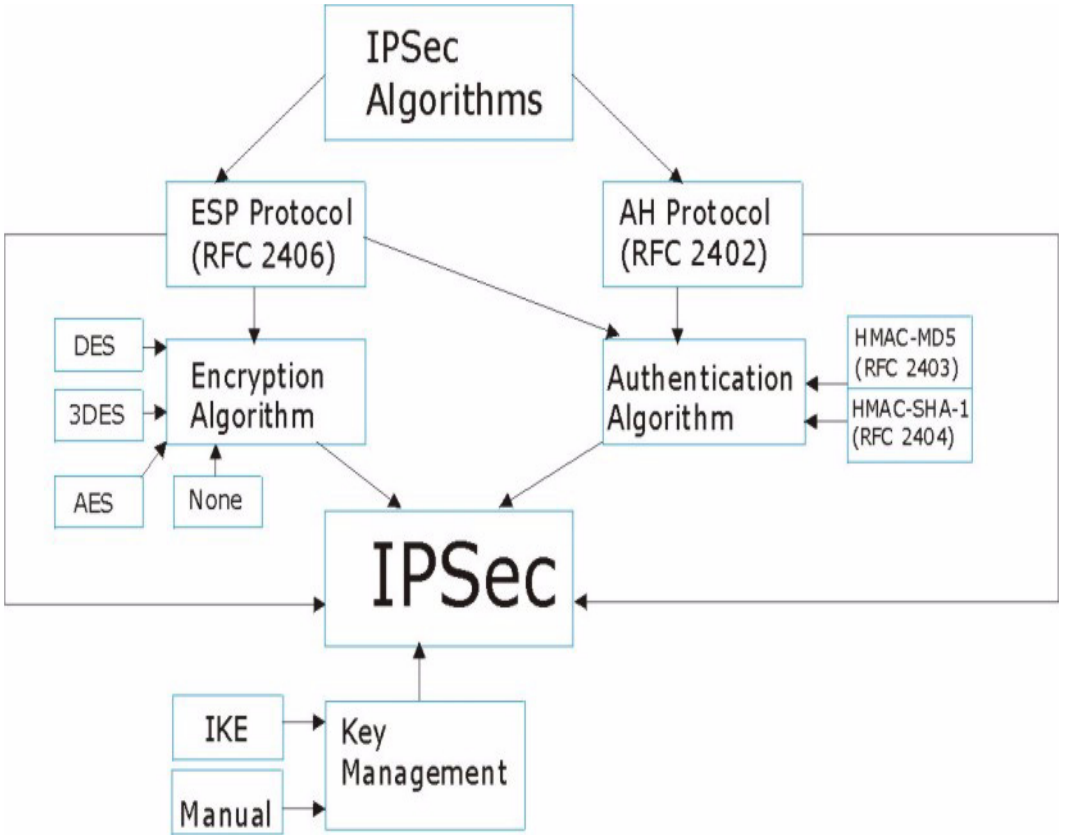
- Unsupported IP Applications

  A VPN tunnel can be created to add support for unsupported emerging IP applications.

IPSec architecture

The overall IPSec architecture is shown as follows in Figure 65.

Figure 65 IPSec architecture



IPSec algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols.

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. After the SA is established, the transport of data can commence.

AH (Authentication Header) protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but can be used for verification of the integrity of the information and authentication of the originator.

ESP (Encapsulating Security Payload) protocol

The **ESP** protocol (RFC 2406) provides encryption, as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the exclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 47 AH and ESP

	ESP	**AH**
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data during phase 1. You can configure the device to use a 128-bit, 192-bit or 256-bit key for phase 2. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

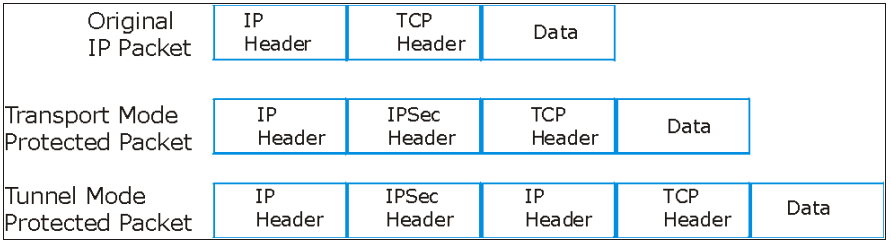
Key management

Your Business Secure Router uses IKE (ISAKMP) key management in order to set up a VPN.

Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 66 Transport and Tunnel mode IPSec encapsulation



Transport mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for VPN switch to VPN switch and host to VPN switch communications. **Tunnel** mode communications have two sets of IP headers:

Outside header: The outside IP header contains the destination IP address of the VPN switch.

Inside header: The inside IP header contains the destination IP address of the final system behind the VPN switch. The security protocol appears after the outer IP header and before the inside IP header.

IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Business Secure Router.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints rewrites either the source or destination address with one of its own choosing. The VPN device at the receiving end verifies the integrity of the incoming packet by computing its own hash value, and complains that the hash value appended to the received packet does not match. The VPN device at the receiving end does not know about the NAT in the middle, so it assumes that the data was maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN switch, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the original header plus original payload, which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see "NAT Traversal" on page 215 for details).

Table 48 VPN and NAT

Security Protocol	Mode	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote VPN switch (secure gateway). You can specify this for a VPN rule in the **VPN Branch Office Rule Setup** screen (see Figure 72 on page 223).

If the remote VPN switch has a static WAN IP address, enter it in the **Secure Gateway Address** field. You can alternatively enter the remote VPN switch's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote VPN switch's domain name in the **Secure Gateway Address** field if the remote VPN switch has a dynamic WAN IP address and is using DDNS. The Business Secure Router has to rebuild the VPN tunnel each time the remote VPN switch's WAN IP address changes (there can be a delay until the DDNS servers are updated with the remote VPN switch's new WAN IP address).

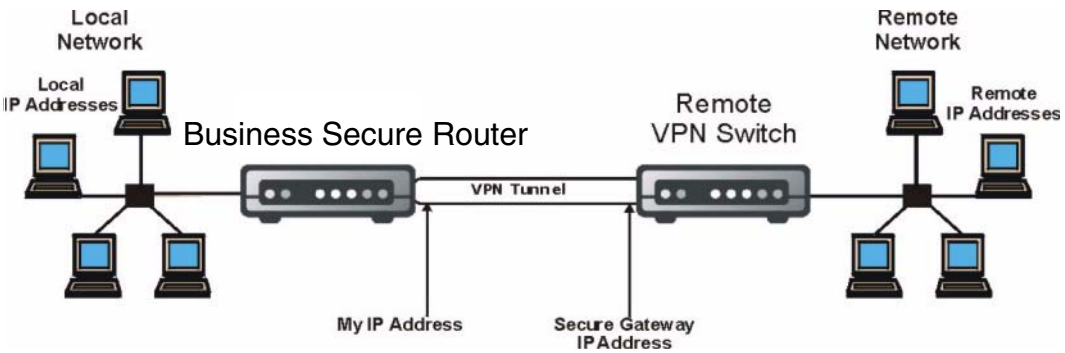
Dynamic Secure Gateway Address

If the remote VPN switch has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the remote VPN switch's address. In this case, only the remote VPN switch can initiate SAs. This is useful for telecommuters initiating a VPN tunnel to the company network.

Summary screen

Figure 67 helps explain the main fields in the WebGUI.

Figure 67 IPSec summary fields

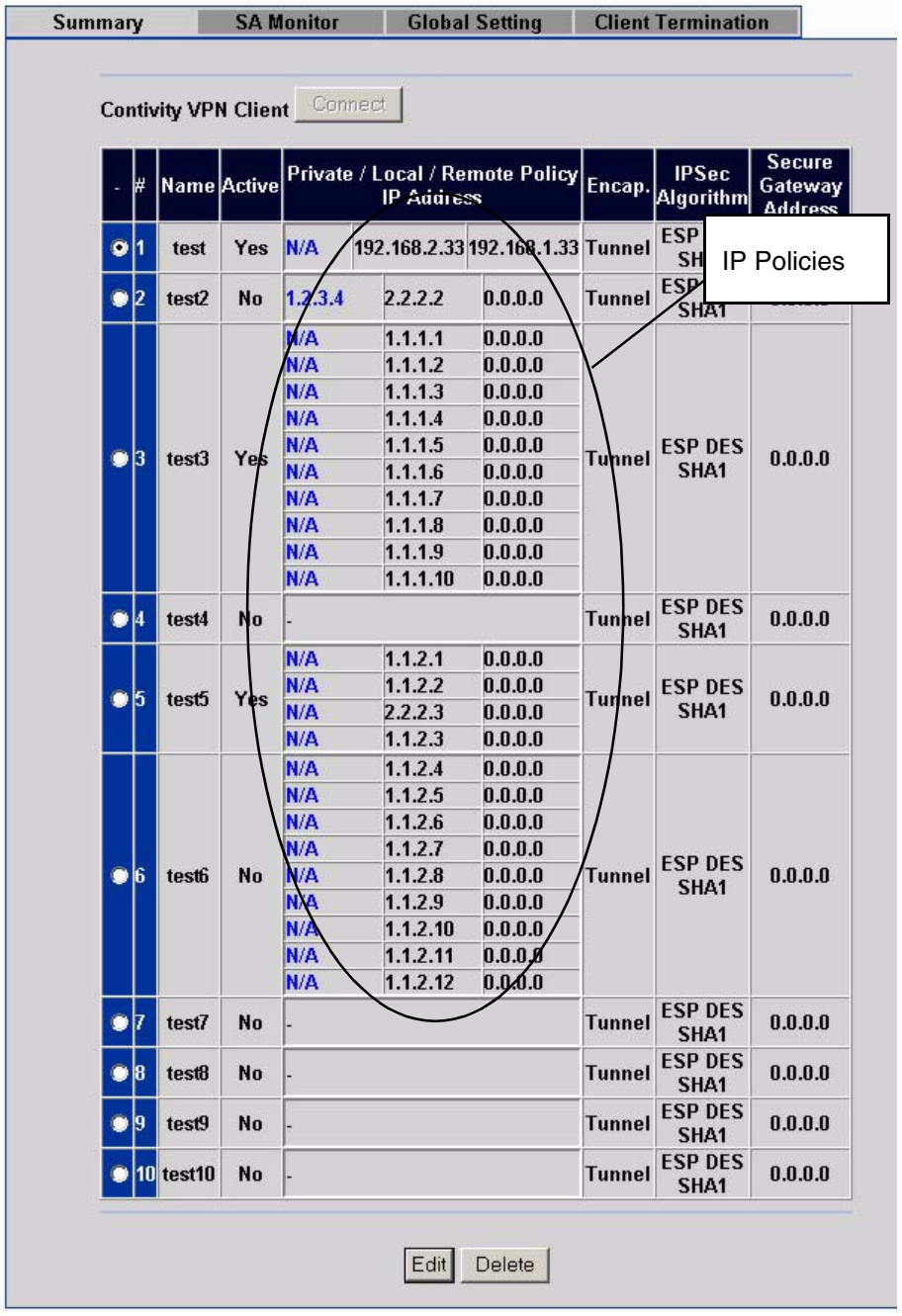


Click **VPN** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

The firewall allows traffic to go through your VPN tunnels.

Figure 68 Summary

VPN



-	#	Name	Active	Private / Local / Remote Policy IP Address			Encap.	IPSec Algorithm	Secure Gateway Address
◉	1	test	Yes	N/A	192.168.2.33	192.168.1.33	Tunnel	ESP SH	
○	2	test2	No	1.2.3.4	2.2.2.2	0.0.0.0	Tunnel	ESP SHA1	
○	3	test3	Yes	N/A	1.1.1.1	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0
				N/A	1.1.1.2	0.0.0.0			
				N/A	1.1.1.3	0.0.0.0			
				N/A	1.1.1.4	0.0.0.0			
				N/A	1.1.1.5	0.0.0.0			
				N/A	1.1.1.6	0.0.0.0			
				N/A	1.1.1.7	0.0.0.0			
				N/A	1.1.1.8	0.0.0.0			
				N/A	1.1.1.9	0.0.0.0			
				N/A	1.1.1.10	0.0.0.0			
○	4	test4	No	-			Tunnel	ESP DES SHA1	0.0.0.0
○	5	test5	Yes	N/A	1.1.2.1	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0
				N/A	1.1.2.2	0.0.0.0			
				N/A	2.2.2.3	0.0.0.0			
				N/A	1.1.2.3	0.0.0.0			
○	6	test6	No	N/A	1.1.2.4	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0
				N/A	1.1.2.5	0.0.0.0			
				N/A	1.1.2.6	0.0.0.0			
				N/A	1.1.2.7	0.0.0.0			
				N/A	1.1.2.8	0.0.0.0			
				N/A	1.1.2.9	0.0.0.0			
				N/A	1.1.2.10	0.0.0.0			
				N/A	1.1.2.11	0.0.0.0			
				N/A	1.1.2.12	0.0.0.0			
○	7	test7	No	-			Tunnel	ESP DES SHA1	0.0.0.0
○	8	test8	No	-			Tunnel	ESP DES SHA1	0.0.0.0
○	9	test9	No	-			Tunnel	ESP DES SHA1	0.0.0.0
○	10	test10	No	-			Tunnel	ESP DES SHA1	0.0.0.0

Table 49 describes the fields in Figure 68.

Table 49 Summary

Label	Description
Contivity VPN Client	The Contivity VPN Client is a simple VPN rule that lets you define and store connection information for accessing your corporate network through a VPN switch. The Contivity VPN Client uses the IPSec protocol to establish a secure end-to-end connection. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive. When this button displays **Connect**, click it to create a VPN connection to the remote Contivity switch. When this button displays **Disconnect**, click it to drop the Contivity VPN connection.
#	This is the VPN rule index number.
Name	This field displays the name you specified in the **VPN Branch Office Rule Setup** screen to identify this VPN policy.
Active	This field displays whether the VPN rule is active or not. A **Yes** signifies that this VPN rule is active. **No** signifies that this VPN rule is not active.
Private /Local / Remote Policy IP Address	These are the IP addresses of the computers that can use the VPN tunnel. Ranges of IP addresses are indicated by the starting and ending IP addresses separated by a dash. You configure these IP addresses in the **VPN Branch Office IP Policy** screen. This field is empty if you do not configure the VPN branch office rule to use an IP policy. Private IP addresses are IP addresses of computers on your Business Secure Router's local network, for which you have configured the IP policy to use NAT for the VPN tunnel. Local IP addresses are the IP addresses of the computers on your Business Secure Router's local network that can use the VPN tunnel. Remote IP addresses are the IP addresses of the computers behind the remote VPN switch that can use the VPN tunnel. When **0.0.0.0** displays, only the remote VPN switch can initiate the VPN. The address **0.0.0.0** displays when the **Secure Gateway Address** field is configured to **0.0.0.0** or the IP policy's **Remote Starting IP Address** field is set to **0.0.0.0** in the **IP Policy** screen.
Encap	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase Business Secure Router processing requirements and communications latency (delay).
Secure Gateway Address	This is the static WAN IP address or URL of the remote VPN switch. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **VPN Branch Office** screen to **0.0.0.0.**

Table 49 Summary

Label	Description
Edit	Click the radio button next to a VPN index number and then click **Edit** to edit a specific VPN policy.
Delete	Click the radio button next to a VPN policy number you want to delete and then click **Delete**. When a VPN policy is deleted, subsequent policies do not move up in the page list.

Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the Business Secure Router automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see "Configuring advanced Branch office setup" on page 241 section for more information about the IPSec SA lifetime). The keep alive option is available with the Contivity Client rule. See the **VPN Contivity Client Rule Setup** screen (Figure 70 on page 217). In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both VPN switches must have a Business Secure Router compatible keep alive feature enabled in order for this feature to work.

If the Business Secure Router has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the Business Secure Router because the Business Secure Router does not drop the tunnels that are already connected (unless there is outbound traffic with no inbound traffic).

Note: No matter whether or not keep alive is set, when there is outbound traffic with no inbound traffic, the Business Secure Router automatically drops the tunnel after two minutes.

Nailed Up

The nailed up feature is similar to the keep alive feature. When you initiate an IPSec tunnel with nailed up enabled, the Business Secure Router automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see "Configuring advanced Branch office setup" on page 241 for more information about the IPSec SA lifetime). The nailed up option is available with the branch

office rules. See the **VPN Branch Office Rule Setup** screen (Figure 72 on page 223). Unlike keep alive, any time the Business Secure Router restarts, it also automatically renegotiates any nailed up tunnels. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Also different from keep alive, the peer VPN switch does not have to have a Business Secure Router compatible nailed up feature enabled in order for this feature to work.

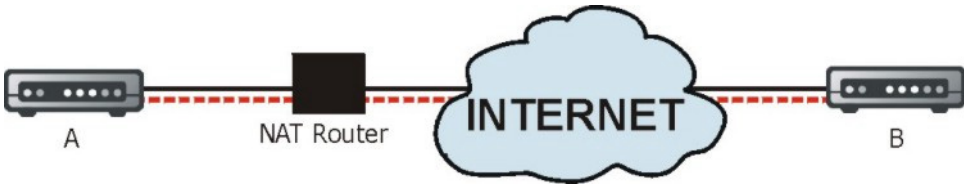
If the Business Secure Router has its maximum number of simultaneous IPSec tunnels connected to it and they all have nailed up enabled, no other tunnels can take a turn connecting to the Business Secure Router because the Business Secure Router does not drop the tunnels that are already connected (unless there is outbound traffic with no inbound traffic).

Note: No matter whether or not nailed up is set, when there is outbound traffic with no inbound traffic, the Business Secure Router automatically drops the tunnel after two minutes.

NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the Nortel Business Secure Router 222 and the remote VPN switch.

Figure 69 NAT router between VPN switches



Normally, you cannot set up a VPN connection with a NAT router between the two VPN switches because the NAT router changes the header of the IPSec packet. In the previous figure, VPN switch A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet’s header so it does not match the header for which VPN switch B is checking. Therefore, VPN switch B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. VPN switch B checks the UDP port 500 header and responds. VPN switches A and B build a VPN connection.

NAT Traversal configuration

Enable or disable NAT traversal in the **VPN Branch Office Rule Setup** screen (see Figure 72 on page 223). For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode)
- Use IKE keying mode
- Enable NAT traversal on both IPSec endpoints

In order for VPN switch A (see Figure 72 on page 223) to receive an initiating IPSec packet from VPN switch B, set the NAT router to forward UDP port 500 to VPN switch A.

Preshared key

A preshared key identifies a communicating party during a phase 1 IKE negotiation (see "IKE phases" on page 238 for more information). It is called preshared because you have to share it with another party before you can communicate with them over a secure connection. For Contivity Client VPN connections, the Business Secure Router generates the preshared key from the username and password.

Configuring Contivity Client VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. The **VPN Contivity Client Rule Setup** screen is shown in Figure 70.

Figure 70 VPN Contivity Client rule setup

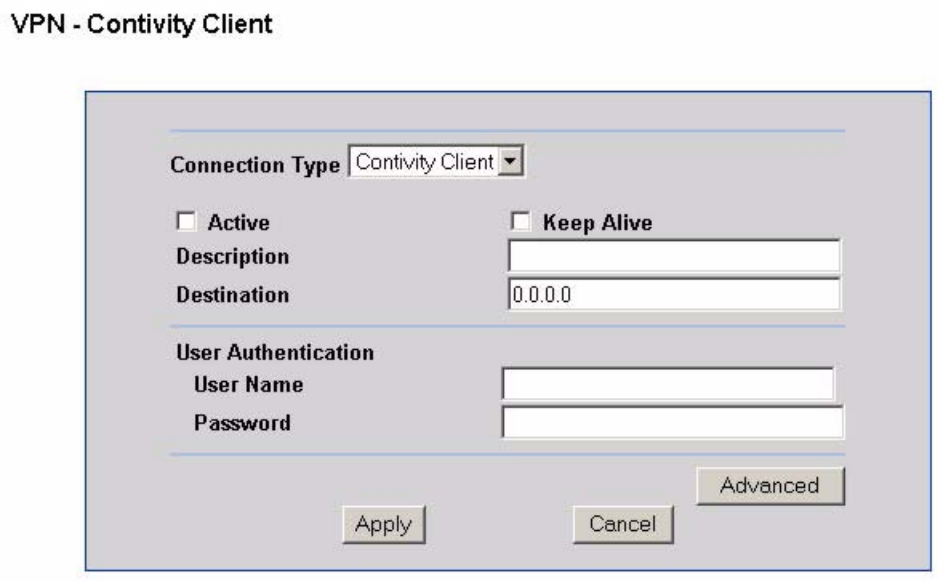


Table 50 VPN Contivity Client rule setup

Label	Description
Connection Type	Select **Branch Office** to manually configure a VPN rule. This has the Nortel Business Secure Router 222 operate as a VPN router. Select **Contivity Client** to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a VPN switch. This has the Nortel Business Secure Router 222 operate as a VPN client.
Active	Select this check box to turn on this rule. Clear this check box if you do not want to use this rule after you apply it. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive. To set a Contivity Client rule to active, all of the other VPN rules must be disabled.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA. Turn on Keep Alive to have the Business Secure Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote VPN switch must also have keep alive enabled in order for this feature to work.
Description	Enter a brief description about this rule for identification purposes.

Table 50 VPN Contivity Client rule setup

Label	Description
Destination	This field specifies the IP address or the domain name (up to 31 case-sensitive characters) of the remote VPN switch. You can use alphanumeric characters, the underscore, dash, period and the @ symbol in a domain name. No spaces are allowed.
User Name	Enter the username exactly as the VPN switch administrator gives it to you.
Password	Enter the password exactly as the VPN switch administrator gives it to you.
Advanced	Click **Advanced** to configure group authentication and on-demand client tunnel settings.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to return to the **VPN Summary** screen without saving your changes.

Configuring Advanced Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. Click **Advanced** to display the **VPN Contivity Client Advanced Rule Setup** screen as shown in Figure 71.

Figure 71 VPN Contivity Client advanced rule setup

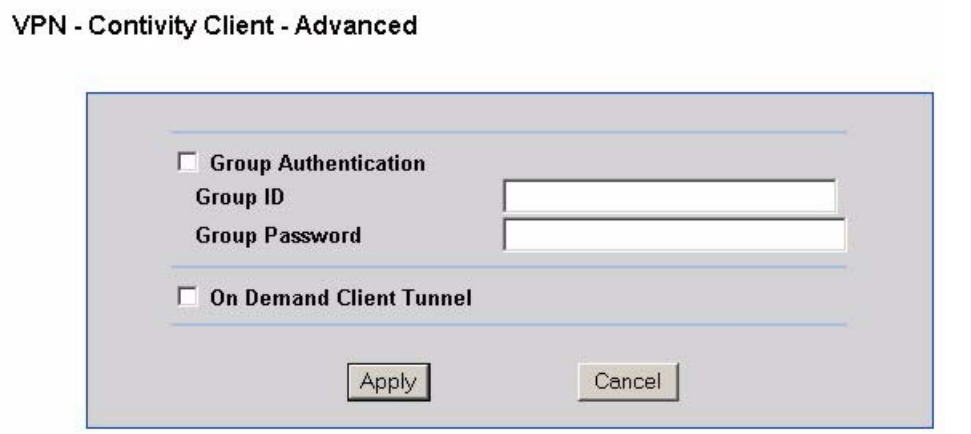


Table 51 describes the fields in Figure 71.

Table 51 VPN Contivity Client advanced rule setup

Label	Description
Group Authentication	Enable **Group Authentication** to have the Business Secure Router send a **Group ID** and **Group Password** to the remote VPN switch for initial authentication. After a successful initial authentication, a RADIUS server associated with the remote VPN switch uses the **User Name** and **Password** to authenticate the Business Secure Router. You must also configure the **Group ID** and **Group Password** fields when you enable **Group Authentication**. After **Group Authentication** is not enabled, the remote VPN switch uses the **User Name** and **Password** to authenticate the Business Secure Router.
Group ID	Enter the group ID exactly as the VPN switch administrator gives it to you. This field only applies when you enable **Group Authentication**.
Group Password	Enter the group password exactly as the VPN switch administrator gives you. This field only applies when you enable **Group Authentication**.
On Demand Client Tunnel	Select this check box to have any outgoing packets automatically trigger a VPN connection to the remote VPN switch. When **On Demand Client Tunnel** is not enabled, you need to go to the **VPN Summary** screen and click the **Connect** button to create a VPN connection to the remote VPN switch.
Apply	Click **Apply** to temporarily save the settings and return to the **VPN - Contivity Client** screen. The **Group Authentication** settings are saved to the Business Secure Router if you click **Apply** in the **VPN - Contivity Client** screen.
Cancel	Click **Cancel** to return to the **VPN Contivity Client Rule Setup** screen without saving your changes.

Note: Click Apply in the VPN - Contivity Client screen to save the Group Authentication settings.

ID Type and content

With aggressive negotiation mode (see "Negotiation Mode" on page 239 for more information), the Business Secure Router identifies incoming SAs by ID type and content since this identifying information is not encrypted, so that is can distinguish between multiple rules for SAs that connect from remote VPN switches that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Business Secure Router from VPN switches with dynamic IP addresses.

Note: Regardless of the ID type and content configuration, you cannot save multiple active rules with overlapping local and remote IP addresses with the Business Secure Router.

With the main negotiation mode (see "Negotiation Mode" on page 239 for more information), the ID type and content are encrypted to provide identity protection. In this case the Business Secure Router can only distinguish between up to 12 different incoming SAs that connect from remote VPN switches that have dynamic WAN IP addresses. The Business Secure Router can distinguish up to 12 incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and three key groups (DH1, DH2, and DH5) when you configure a VPN rule (see "Configuring advanced Branch office setup" on page 241). The ID type and content act as an extra level of identification for incoming SAs.

Configure the ID type and content in the **VPN Branch Office Rule Setup** screen (see Figure 72 on page 223). The type of ID can be a domain name, an IP address, or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 52 Local ID type and content fields

Local ID type=	Content=
IP	Type the IP address of your computer or leave the field blank to have the Business Secure Router automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Business Secure Router.

Table 52 Local ID type and content fields

Local ID type=	Content=
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Business Secure Router.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 53 Peer ID type and content fields

Peer ID type=	Content=
IP	Type the IP address of the computer with which you make the VPN connection or leave the field blank to have the Business Secure Router automatically use the address in the **Secure Gateway** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote VPN switch.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote VPN switch.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote VPN switch's IP address or what you configure in the **Secure Gateway Address** field below.	

ID type and content examples

Two VPN switches must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Business Secure Routers shown in Table 54 can complete negotiation and establish a VPN tunnel.

Table 54 Matching ID type and content configuration example

Business Secure Router A	Business Secure Router B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two Business Secure Routers shown in Table 55 cannot complete their negotiation because Business Secure Router B's **Local ID type** is **IP**, but Business Secure Router A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 55 Mismatching ID Type and Content Configuration Example

Business Secure Router A	Business Secure Router B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

My IP Address

My IP Address is the WAN IP address of the Business Secure Router. The Business Secure Router has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

The following applies if this field is configured as 0.0.0.0:

- The Business Secure Router uses the current Business Secure Router WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the Business Secure Router uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See Chapter 7, "WAN screens," on page 105 for details about dial backup and traffic redirect.

Configuring Branch Office VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The **VPN Branch Office Rule Setup** screen is shown in Figure 72.

Figure 72 VPN Branch Office rule setup

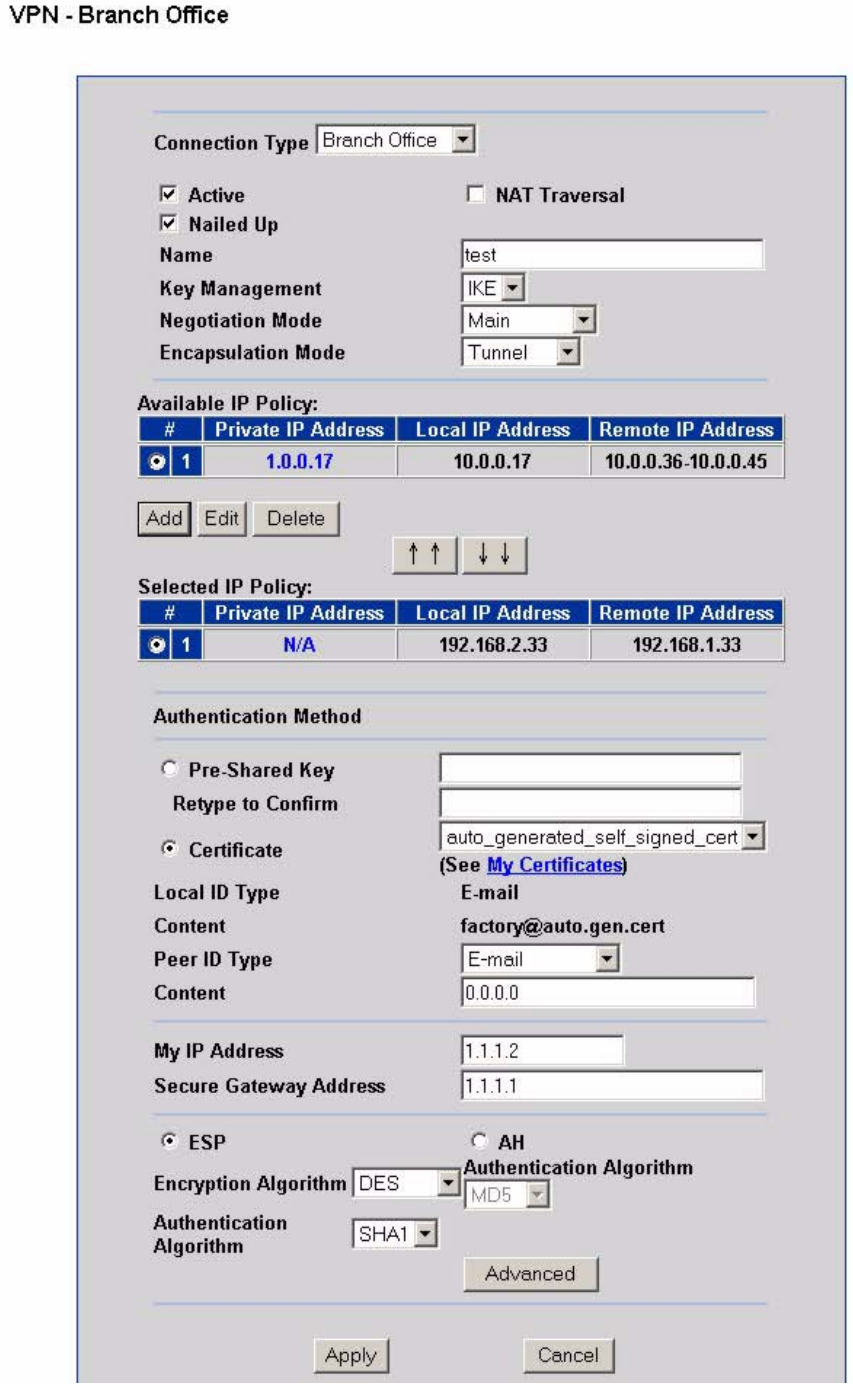


Table 56 describes the fields in Figure 72.

Table 56 VPN Branch Office rule setup

Label	Description
Connection Type	Select **Branch Office** to manually configure a VPN rule. Select **Contivity Client** to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a VPN switch. You can only configure one Contivity client rule. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied.
Nailed Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the Business Secure Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The Business Secure Router also reinitiates the SA when it restarts.
NAT Traversal	Select this check box to enable NAT traversal. With NAT traversal, you can set up a VPN connection when there are NAT routers between the two VPN switches. The remote VPN switch must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol. In order for a VPN switch behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the VPN switch behind the NAT router.
Name	Type a name to identify this VPN policy. You can use any character, including spaces, but the Business Secure Router drops trailing spaces.
Key Management	Your Business Secure Router uses IKE (ISAKMP) key management in order to set up a VPN.
Negotiation Mode	Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords. Multiple SAs connecting through a VPN switch must have the same negotiation mode.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list. **Tunnel** is compatible with NAT, **Transport** is not.

Table 56 VPN Branch Office rule setup

Label	Description
Available/ Selected IP Policy	The **Available IP Policy** table displays network routes. Use the **Add**, **Edit** and **Delete** buttons to configure this list. Move the network routes that you want to use the VPN tunnel down into the **Selected IP Policy** table. Select a network route's radio button in the **Available IP Policy** table, then click the down arrows to move it into the **Selected IP Policy** table. To remove a network route from the **Selected IP Policy** table, select its radio button in the **Selected IP Policy** table and click the up arrows. A network route that is already selected for a VPN tunnel does not display in the **Available IP Policy** table.
Private IP Address	This field displays the IP address (or a range of IP addresses) of the computers on your Business Secure Router's local network, for which you have configured this VPN rule. For a range of addresses, the starting and ending IP addresses are displayed separated by a dash. This field applies when you configure the IP policy to use a branch tunnel NAT address mapping rule in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-One** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many-to-One** or **Many One-to-one** in the **IP Policy** screen.

Table 56 VPN Branch Office rule setup

Label	Description
Local IP Address	This field displays the IP address (or range of IP addresses) of the computers on your Business Secure Router's local network, for which you have configured this IP policy. This field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-one** or **Many-to-One** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many One-to-one** in the **IP Policy** screen. This field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Local Address Type** field is configured to **Single Address** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Local Address Type** field is configured to **Range Address** in the **IP Policy** screen. This field displays a (static) IP address and a subnet mask when the IP policy's **Local Address Type** field is configured to **Subnet Address** in the **IP Policy** screen.

Table 56 VPN Branch Office rule setup

Label	Description
Remote IP Address	This field displays the IP addresses of computers on the remote network behind the remote VPN switch. This field displays a single (static) IP address when the IP policy's **Remote Address Type** field is configured to **Single Address** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Remote Address Type** field is configured to **Range Address** in the **IP Policy** screen. This field displays a (static) IP address and a subnet mask when the IP policy's **Remote Address Type** field is configured to **Subnet Address** in the **IP Policy** screen. This field displays **ALL** whenever the **Secure Gateway Address** field is set to **0.0.0.0**. This field also displays **ALL** whenever the IP policy's **Remote Starting IP Address** field is set to **0.0.0.0** in the **IP Policy** screen. When **ALL** displays, only the remote VPN switch can initiate the VPN.
Add	Select **Add** to open a screen where you can configure an IP policy.
Edit	Select the radio button next to an IP policy and then click **Edit** to edit that IP policy.
Delete	Select the radio button next to an IP policy that you want to remove and then click **Delete**.
Authentication Method	Select the **Pre-Shared Key** radio button to use a preshared secret key to identify the Business Secure Router. Select the **Certificate** radio button to identify the Business Secure Router by a certificate.
Preshared Key	Type your preshared key in this field. A preshared key identifies a communicating party during a phase 1 IKE negotiation. It is called preshared because you must share it with another party before you can communicate with that party over a secure connection. Type from 8 to 32 case-sensitive ASCII characters or from 16 to 62 hexadecimal (0-9, A-F) characters. You must precede a hexadecimal key with a 0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in 0x0123456789ABCDEF, “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same preshared key. You see a “PYLD_MALFORMED” (payload malformed) log if the same preshared key is not used on both ends.
Retype to Confirm	Type your preshared key again in this field.

Table 56 VPN Branch Office rule setup

Label	Description
Certificate	Use the drop-down list to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen, where you can view the Business Secure Router's list of certificates.
Local ID Type	Select **IP** to identify this Business Secure Router by its IP address. Select **DNS** to identify this Business Secure Router by a domain name. Select **E-mail** to identify this Business Secure Router by an e-mail address.
Local Content	When you select **IP** in the **Local ID Type** field, type an IP address or leave the field blank to have the Business Secure Router automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Business Secure Router. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this Business Secure Router. The IP address, domain name, or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.
Peer ID Type	Select **IP** to identify the remote VPN switch by its IP address. Select **DNS** to identify the remote VPN switch by a domain name. Select **E-mail** to identify the remote VPN switch by an e-mail address.

Table 56 VPN Branch Office rule setup

Label	Description
Peer Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you make the VPN connection or leave the field blank to have the Business Secure Router automatically use the address in the **Secure Gateway Address** field. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote VPN switch. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote VPN switch. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field. Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.
My IP Address	Enter the WAN IP address of your Business Secure Router. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0** (the default): • The Business Secure Router uses the current Business Secure Router WAN IP address (static or dynamic) to set up the VPN tunnel. • If the WAN connection goes down, the Business Secure Router uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the VPN switch with which you are making the VPN connection. Set this field to **0.0.0.0** if the remote VPN switch has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**). The remote address fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case, only the remote VPN switch can initiate the VPN. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.

Table 56 VPN Branch Office rule setup

Label	Description
ESP	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as the services offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation, but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encryption Algorithm	Select **DES**, **3DES**, **AES 128**, **AES 192**, **AES 256** or **NULL** from the drop-down list. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Advanced	Click **Advanced** to go to a screen where you can configure detailed IKE (Internet Key Exchange) negotiation–phase 1 (Authentication) and phase 2 (Key Exchange) settings for the rule.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to return to the **VPN Summary** screen without saving your changes.

Configuring an IP Policy

Select one of the IP policies in the **VPN Branch Office** screen and click **Add** or **Edit** to configure the policy's settings. The **Branch Office – IP Policy** setup screen is shown in Figure 73.

Figure 73 VPN Branch Office — IP Policy

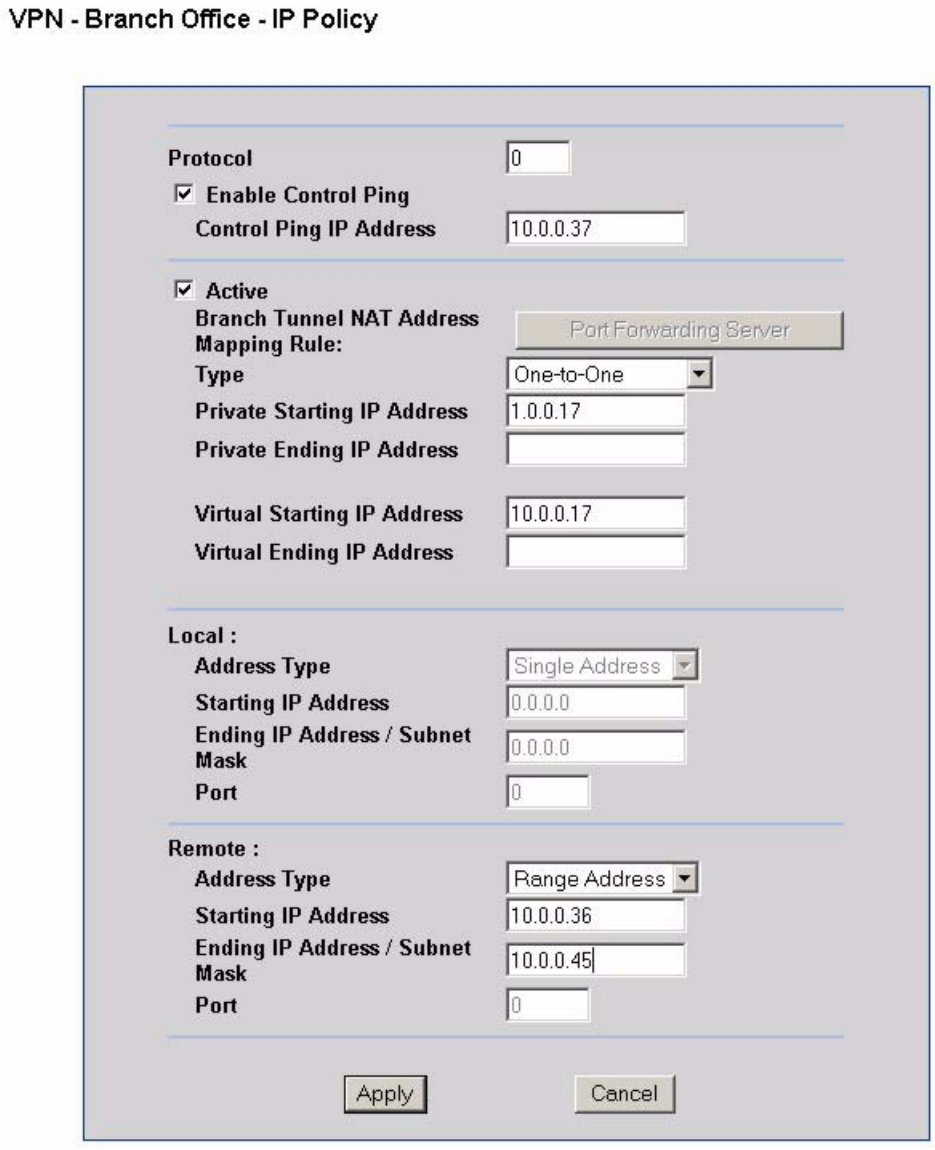


Table 57 describes the fields in Figure 73.

Table 57 VPN Branch Office — IP Policy

Label	Description
Protocol	Enter a number to specify what type of traffic is allowed to go through the VPN tunnel that is built using this IP policy. Use 1 for ICMP, 6 for TCP, 17 for UDP, and so on. 0 is the default and signifies any protocol. For example, if you select 1 (ICMP), only ICMP packets can go through the tunnel. If you specify a protocol other than 1 (ICMP) or 0 (any protocol), you cannot use the control ping feature. If you set this field to 6 (TCP) or 17 (UDP), you can use the **Port** field to specify the port number of the allowed traffic.
Enable Control Ping	Select the check box and configure an IP address in the **Control Ping IP Address** field to have the Business Secure Router periodically test the VPN tunnel to the branch office. The Business Secure Router pings the IP address every minute. The Business Secure Router starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote VPN switch by the time the timeout period expires, the Business Secure Router disconnects the VPN tunnel.
Control Ping IP Address	If you select **Enable Control Ping**, enter the IP address of a computer at the branch office. The computer's IP address must be in this IP policy's remote range (see the **Remote** fields).
Branch Tunnel NAT Address Mapping Rule	
Port Forwarding Server	Click **Port Forwarding Server** to configure a list of inside (behind NAT on the LAN) servers, for example, web or FTP. The Business Secure Router makes these servers visible to the devices using the VPN branch NAT tunnel (from behind the remote VPN switch) even though NAT makes your inside network appear as a single machine. This option applies when the **Type** field is configured to **Many-to-One**.
Active	Enable this feature to have the Business Secure Router use a different (virtual) IP address for the VPN connection. When you enable branch tunnel NAT address mapping, you do not configure the local section.

Table 57 VPN Branch Office — IP Policy

Label	Description
Type	Select one of the following port mapping types. 1. **One-to-One**: One-to-one mode maps one private IP address to one virtual IP address. Port numbers do not change with one-to-one NAT mapping. 2. **Many-to-One**: Many-to-One mode maps multiple private IP addresses to one virtual IP address. This is equivalent to SUA (for example, PAT, port address translation), Business Secure Router's Single User Account feature. 3. **Many One-to-one**: Many One-to-one mode maps each private IP address to a unique virtual IP address. Port numbers do not change with many one-to-one NAT mapping.
Private Starting IP Address	When the **Type** field is configured to **One-to-one**, enter the (static) IP address of the computer on your Business Secure Router's LAN that is to use the VPN tunnel. When the **Type** field is configured to **Many-to-One** or **Many One-to-one**, enter the beginning (static) IP address of the range of computers on your Business Secure Router's LAN that are to use the VPN tunnel.
Private Ending IP Address	When the **Type** field is configured to **One-to-one**, this field is N/A. When the **Type** field is configured to **Many-to-One** or **Many One-to-one**, enter the ending (static) IP address of the range of computers on your Business Secure Router's LAN that are to use the VPN tunnel.
Virtual Starting IP Address	Virtual addresses must be static and correspond to the remote VPN switch's configured remote IP addresses. The computers on the Business Secure Router's LAN and the remote network can function as if they were on the same subnet when the virtual IP address(es) is on the same subnet as the remote IP addresses. Two active SAs can have the same virtual or remote IP address, but not both. You can configure multiple SAs between the same virtual and remote IP addresses, as long as only one is active at a time. When the **Type** field is configured to **One-to-one** or **Many-to-One**, enter the (static) IP address that you want to use for the VPN tunnel. When the **Type** field is configured to **Many One-to-one**, enter the beginning (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.

Table 57 VPN Branch Office — IP Policy

Label	Description
Virtual Ending IP Address	When the **Type** field is configured to **One-to-one** or **Many-to-One**, this field is N/A. When the **Type** field is configured to **Many One-to-one**, enter the ending (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.
Local	Local IP addresses must be static and correspond to the remote VPN switch's configured remote IP addresses. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at a time. Two IP policies can have the same local or remote IP address, but not both. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your Business Secure Router. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Business Secure Router. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your Business Secure Router.
Ending IP Address / Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your Business Secure Router. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your Business Secure Router.

Table 57 VPN Branch Office — IP Policy

Label	Description
Protocol	Enter a number to specify what type of traffic is allowed to go through the VPN tunnel that is built using this IP policy. Use 1 for ICMP, 6 for TCP, 17 for UDP, and so on. 0 is the default and signifies any protocol. For example, if you select 1 (ICMP), only ICMP packets can go through the tunnel. If you specify a protocol other than 1 (ICMP) or 0 (any protocol), you cannot use the control ping feature. If you set this field to 6 (TCP) or 17 (UDP), you can use the **Port** field to specify the port number of the allowed traffic.
Port	This field is available when you set the Protocol field to 6 (TCP) or 17 (UDP). Use this field to specify the port number of the traffic that is allowed to go through the VPN tunnel that is built using this IP policy. The default is 0 and it signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. Do this if you want to allow only traffic of a particular port number to go through the VPN tunnel. For example, if you only wanted to allow FTP traffic to go through the VPN tunnel, specify 6 (TCP) in the **Protocol** field and 21 (FTP) in the **Port** field.
Remote	Remote IP addresses must be static and correspond to the remote VPN switch's configured local IP addresses. The remote fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case, only the remote VPN switch can initiate the VPN. Two active SAs cannot have the local and remote IP addresses both the same. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Two IP policies can have the same local or remote IP address, but not both.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your Business Secure Router. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Business Secure Router. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your Business Secure Router.

Table 57 VPN Branch Office — IP Policy

Label	Description
Ending IP Address / Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your Business Secure Router. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your Business Secure Router.
Port	By default, 0 signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to return to the **VPN Branch Office** screen without saving your changes.

Port forwarding server

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the devices using the VPN branch NAT tunnel (from behind the remote VPN switch) even though NAT makes your inside network appear as a single machine. The servers must be using the VPN branch NAT tunnel (from behind the Business Secure Router).

You can enter a single port or a range of ports to be forwarded and then the local IP address of the desired inside servers.

Configuring a port forwarding server

Select one of the IP Policies in the **VPN Branch Office** screen and click **Edit** to display the **Branch Office – IP Policy** setup screen. For the Mapping Rule Type, select **Many-to-One**, enter the private and virtual IP addresses and click the **Port Forwarding Server** button to display the screen shown in Figure 74.

Figure 74 VPN Branch Office — IP Policy - Port Forwarding Server

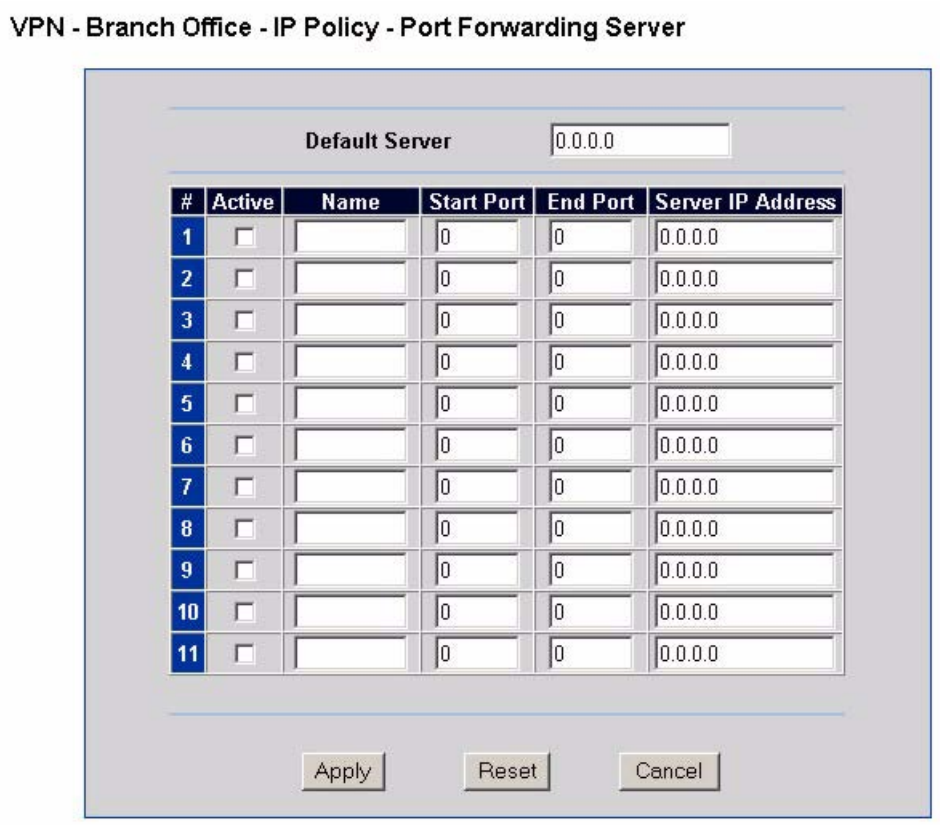


Table 58 describes the fields in Figure 74.

Table 58 VPN Branch Office — IP Policy - Port Forwarding Server

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded.
#	Number of an individual port forwarding server entry.
Active	Select this check box to activate the port forwarding server entry.
Name	Enter a descriptive name for identifying purposes.

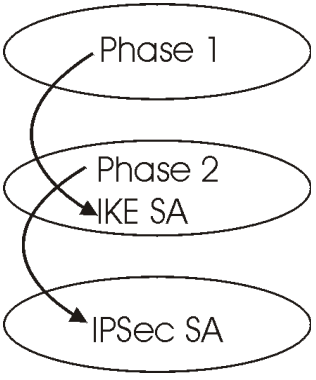
Table 58 VPN Branch Office — IP Policy - Port Forwarding Server

Label	Description
Start Port	Type a port number in this field. To forward only one port, type the port number again in the **End Port** field. To forward a series of ports, type the start port number here and the end port number in the **End Port** field.
End Port	Type a port number in this field. To forward only one port, type the port number in the **Start Port** field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Type your server IP address in this field.
Apply	Click this button to save these settings and return to the **VPN Branch Office - IP Policy** screen.
Reset	Click this button to begin configuring this screen afresh.
Cancel	Click this button to return to the **VPN Branch Office - IP Policy** screen without saving your changes.

IKE phases

There are two phases to every IKE (Internet Key Exchange) negotiation–phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 75 Two phases to set up the IPSec SA



In Phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a preshared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1**, **DH2**, and **DH5**).
- Set the IKE SA lifetime. In this field you can determine how long an IKE SA will stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In Phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography–see "Perfect Forward Secrecy (PFS)" on page 240. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. In this field, you can determine how long the IPSec SA will stay up before it times out. The Business Secure Router automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Business Secure Router also automatically renegotiates the IPSec SA if both VPN switches have keep alive enabled, even if there is no traffic. If an IPSec SA times out, the VPN switch must renegotiate the SA the next time someone attempts to send traffic.

Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) is established for each connection through IKE negotiations.

Main Mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange, and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

Aggressive Mode is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use preshared key authentication.

Preshared key

A preshared key identifies a communicating party during a phase 1 IKE negotiation. It is called preshared because you have to share it with another party before you can communicate with the party over a secure connection.

Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**), 1 024-bit (Group 2 – **DH2**) and 1 536-bit (Group 5 - **DH5**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use preshared keys.

Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This can be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Business Secure Router. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which can have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

Configuring advanced Branch office setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The basic IKE rule setup screen displays.

In the **VPN Branch Office Rule Setup** screen, click the **Advanced** button to display the **VPN Branch Office Advanced Rule Setup** screen.

Figure 76 VPN Branch Office advanced rule setup

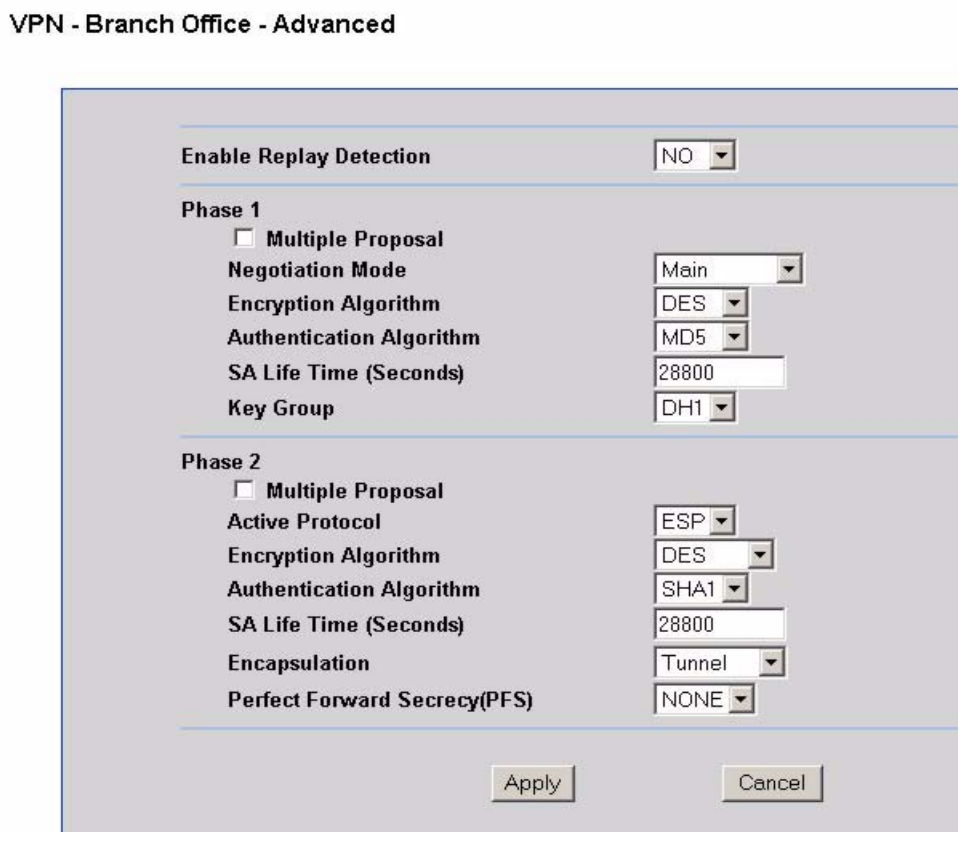


Table 59 describes the fields in Figure 76.

Table 59 VPN Branch Office Advanced Rule Setup

Label	Description
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **YES**.
Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).
Multiple Proposal	Select this check box to allow the Business Secure Router to use any of its phase 1 encryption and authentication algorithms when negotiating an IKE SA. Clear this check box to have the Business Secure Router use only the phase 1 encryption and authentication algorithms configured below when negotiating an IKE SA.
Negotiation Mode	Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords. The Business Secure Router's negotiation mode must be identical to that on the remote VPN switch. Multiple SAs connecting through a VPN switch must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list. The Business Secure Router's authentication algorithm must be identical to the remote VPN switch. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **SHA-1** for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It can range from 60 to 3 000 000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

Table 59 VPN Branch Office Advanced Rule Setup

Label	Description
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1, a 768-bit random number. **DH2** refers to Diffie-Hellman Group 2, a 1 024-bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5, a 1 536-bit random number.
Phase 2	A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.
Multiple Proposal	Select this check box to allow the Business Secure Router to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA. Clear this check box to have the Business Secure Router use only the phase 2 encryption and authentication algorithms when negotiating an IPSec SA.
Active Protocol	Select **ESP** or **AH** from the drop-down list. The Business Secure Router's IPSec Protocol must be identical to the remote VPN switch. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select **ESP** here, you must select options from the Encryption Algorithm and Authentication Algorithm fields. The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation, but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.

Table 59 VPN Branch Office Advanced Rule Setup

Label	Description
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It can range from 60 to 3 000 000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list. The Business Secure Router's encapsulation mode must be identical to the remote VPN switch. **Tunnel** is compatible with NAT, **Transport** is not.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not as secure. Choose from **DH1**, **DH2**, or **DH5** to enable PFS. **DH1** refers to Diffie-Hellman Group 1, a 768-bit random number. **DH2** refers to Diffie-Hellman Group 2, a 1 024-bit (1Kb) random number (more secure, yet slower). **DH5** refers to Diffie-Hellman Group 5, a 1 536-bit random number.
Apply	Click **Apply** to temporarily save the settings and return to the **VPN - Branch Office Rule Setup** screen. The advanced settings are saved to the Business Secure Router if you click **Apply** in the **VPN - Branch Office Rule Setup** screen.
Cancel	Click **Cancel** to return to the **VPN Branch Office** screen without saving your changes.

SA Monitor

In the WebGUI, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage all of the active VPN connections (IPSec sessions).

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. Table 60 describes the fields in this tab.

Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is idle and does not time out until the SA lifetime period expires. See the section "Keep Alive" on page 214 about keep alive to have the Business Secure Router renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 77 VPN SA Monitor

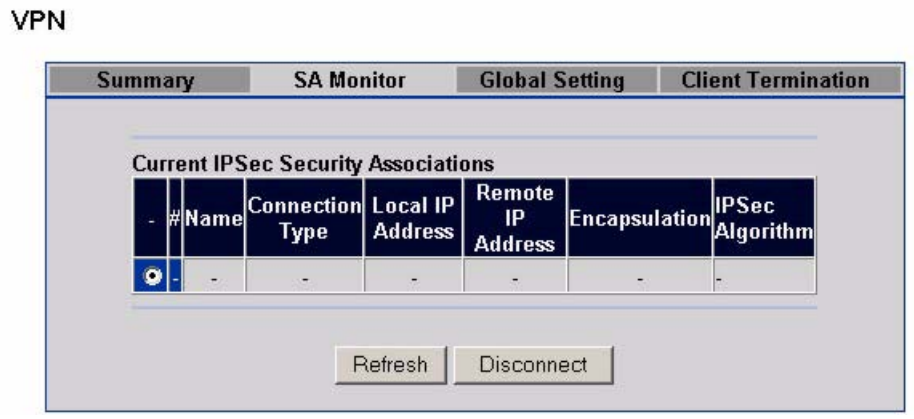


Table 60 describes the fields in Figure 77.

Table 60 VPN SA Monitor

Label	Description
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Connection Type	This field displays whether this is a connection to another IPSec router or to a Contivity VPN client.
Local IP Address	This field displays the IP address of the computer using the VPN IPSec feature of your Business Secure Router.
Remote IP Address	This field displays IP address (in a range) of computers on the remote network behind the remote VPN switch.

Table 60 VPN SA Monitor

Label	Description
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Business Secure Router processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connections. This button is available when you have active VPN connections.
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**. This button is available when you have active VPN connections.
Next Page (if applicable)	Click **Next Page** to view more items in the summary (if you have a summary list that exceeds this page)

Global settings

In the WebGUI, click **VPN** on the navigation panel, then click the **Global Setting** tab.

Figure 78 VPN Global Setting

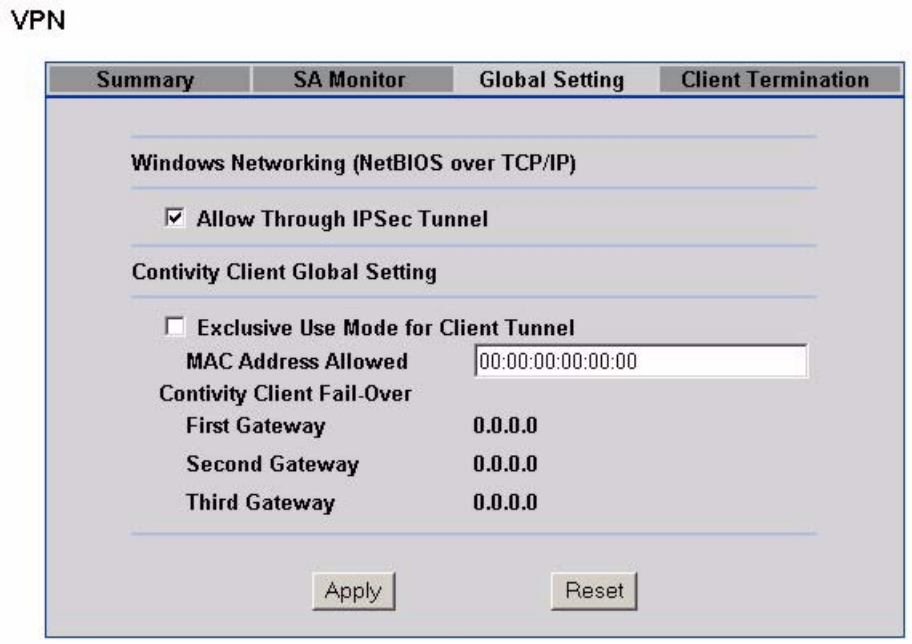


Table 61 describes the fields in Figure 78.

Table 61 VPN Global Setting

Label	Description
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It is sometimes necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Exclusive Use Mode for Client Tunnel	Select this check box to permit only the computer with the MAC address that you specify to set up a VPN connection to the remote VPN switch.
MAC Address Allowed	Enter the MAC address of the computer you want to allow to use the VPN tunnel.

Table 61 VPN Global Setting

Label	Description
Contivity Client Fail-Over	The Contivity Client fail-over feature allows a Contivity client to establish a VPN connection to a backup VPN switch when the default remote VPN switch (specified in the Destination field) is not accessible. The VPN fail-over feature must also be set up in the remote VPN switch.
First Gateway Second Gateway Third Gateway	These read-only fields display the IP addresses of the backup VPN switches. The Business Secure Router automatically gets this information from the default remote VPN switch. After the remote VPN switch is unreachable or fails to respond to IKE negotiation, the Business Secure Router tries to establish a VPN connection to a backup VPN switch.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

VPN Client Termination

Use these screens to configure the Business Secure Router for VPN connections from computers using Nortel's Contivity VPN Client software. In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the screen illustrated in Figure 79. This screen sets the general settings for use with all of the Contivity VPN client tunnels.

Figure 79 VPN Client Termination

VPN

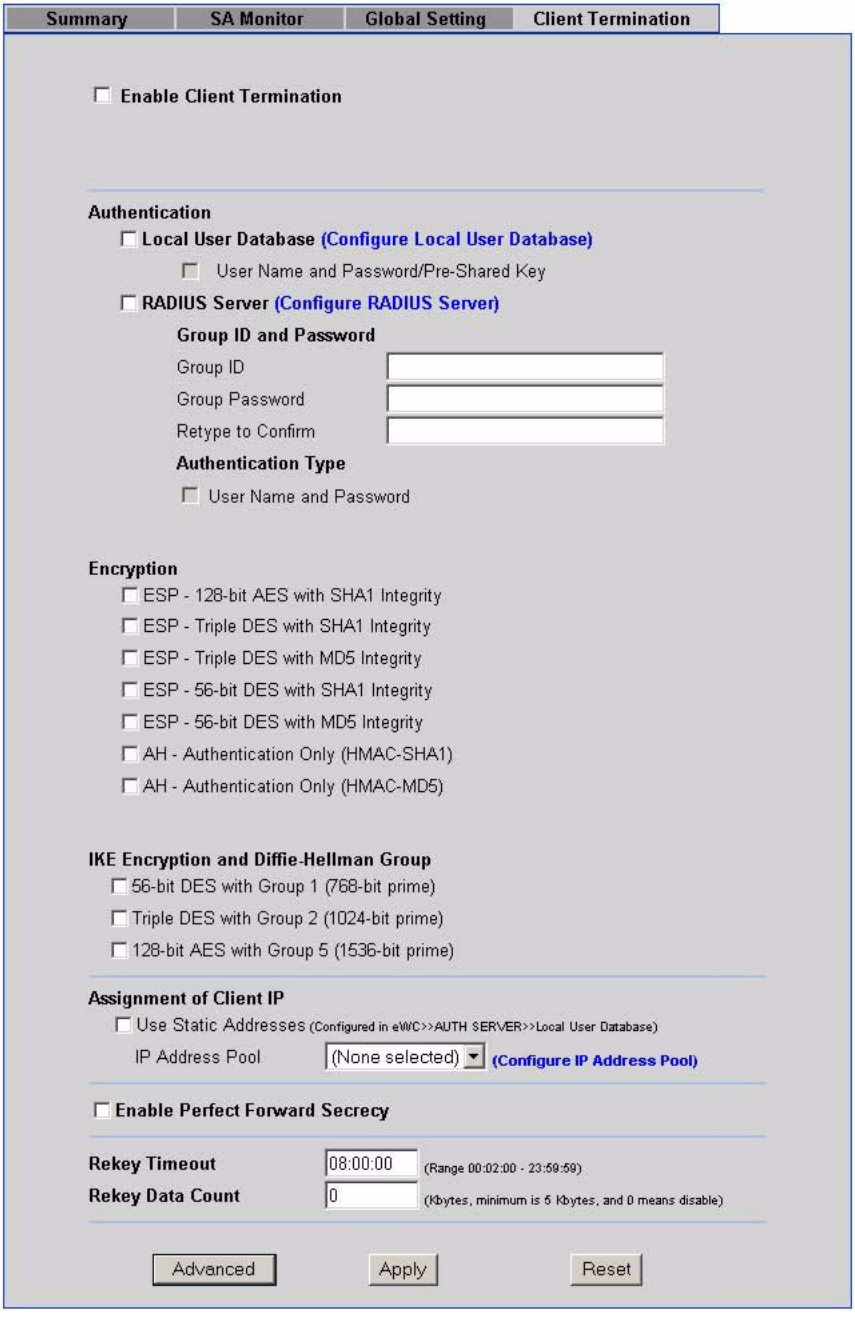

Summary
SA Monitor
Global Setting
Client Termination
Enable Client Termination
Authentication
Local User Database (Configure Local User Database)
User Name and Password/Pre-Shared Key
RADIUS Server (Configure RADIUS Server)
Group ID and Password
Group ID
Group Password
Retype to Confirm
Authentication Type
User Name and Password
Encryption
ESP - 128-bit AES with SHA1 Integrity
ESP - Triple DES with SHA1 Integrity
ESP - Triple DES with MD5 Integrity
ESP - 56-bit DES with SHA1 Integrity
ESP - 56-bit DES with MD5 Integrity
AH - Authentication Only (HMAC-SHA1)
AH - Authentication Only (HMAC-MD5)
IKE Encryption and Diffie-Hellman Group
56-bit DES with Group 1 (768-bit prime)
Triple DES with Group 2 (1024-bit prime)
128-bit AES with Group 5 (1536-bit prime)
Assignment of Client IP
Use Static Addresses (Configured in eWC>>AUTH SERVER>>Local User Database)
IP Address Pool
(None selected)
(Configure IP Address Pool)
Enable Perfect Forward Secrecy
Rekey Timeout
08:00:00
(Range 00:02:00 - 23:59:59)
Rekey Data Count
0
(Kbytes, minimum is 5 Kbytes, and 0 means disable)
Advanced
Apply
Reset

Table 62 describes the fields in Figure 79.

Table 62 VPN Client Termination

Label	Description
Enable Client Termination	Turn on the client termination feature if you want the Business Secure Router to support VPN connections from computers using Contivity VPN Client software.
Local User Database	Select this option to have the Business Secure Router use its internal list of users to authenticate the Contivity VPN clients. Click **Configure Local User Database** to edit the list of users and their usernames and passwords.
User Name and Password/ Pre-Shared Key	Select this option to have the Business Secure Router use the Contivity VPN clients' usernames and passwords as a preshared key to identify them during phase 1 IKE negotiations.
RADIUS Server	Select this option to have the Business Secure Router use an external RADIUS server to identify the Contivity VPN clients during phase 1 IKE negotiations. Click **Configure RADIUS Server** to specify the associated external RADIUS server.
Group ID	The Contivity VPN clients send the group ID and group password to the Business Secure Router for or initial authentication. After a successful initial authentication, the associated external RADIUS server uses the Contivity VPN client's username and password to authenticate the Contivity VPN client. Enter a group ID of up to 31 ASCII characters.
Group Password Retype to Confirm	Enter a group password of up to 31 ASCII characters. Enter it a second time to make sure you have entered it correctly.
Authentication Type	Select **User Name and Password** to have the external RADIUS server use the Contivity VPN clients' usernames and passwords to authenticate them during phase 1 IKE negotiations.

Table 62 VPN Client Termination

Label	Description
Encryption	Select the combinations of protocol and encryption and authentication algorithms that the Business Secure Router is to use for the phase 2 VPN connections (VPN tunnels) with Contivity VPN clients. The ESP (Encapsulation Security Payload) protocol (RFC 2406) uses encryption as well as the services offered by AH. The AH (Authentication Header Protocol) protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation but not for confidentiality, for which the ESP was designed. It does not use encryption. When you use one of the encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES is a variation on DES that uses a 168-bit key. Triple DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit key implementation of AES. AES is faster than 3DES. SHA1 (Secure Hash Algorithm) and MD5 (Message Digest 5) are hash algorithms used to authenticate packet data. SHA1 algorithm is generally considered stronger than MD5, but is slower.
IKE Encryption and Diffie-Hellman Group	Select the combinations of encryption algorithm and Diffie-Hellman key group that the Business Secure Router is to use for phase 1 IKE setup with Contivity VPN clients. The DES encryption algorithm uses a 56-bit key. Triple DES is a variation on DES that uses a 168-bit key. Triple DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit key implementation of AES. AES is faster than 3DES. Diffie-Hellman (DH) is a public-key cryptography protocol that is used within IKE SA setup to establish session keys. The larger the Diffie-Hellman Group, the higher the security. Diffie-Hellman Group 1 uses a 768-bit random number. Diffie-Hellman Group 2 uses a 1 024-bit (1Kb) random number. Diffie-Hellman Group 5 uses a 1 536-bit random number.
Assignment of Client IP	Select **Use Static Addresses** if the Contivity VPN clients are using static IP addresses. You must specify these in the remote user profiles.

Table 62 VPN Client Termination

Label	Description
IP Address Pool	Have the Business Secure Router assign IP addresses to the Contivity VPN clients from a pool of IP address that you define. Select the pool to use. Click **Configure IP Address Pool** to define the ranges of IP addresses that you can select from.
Enable Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) is disabled by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Turn on PFS to use the Diffie-Hellman exchange to create a new key for each IPSec SA setup.
Rekey Timeout	Set the allowed lifetime for an individual key used for data encryption before negotiating a new key. A setting of 00:00:00 disables the rekey timeout.
Rekey Data Count	Set how much data can be transmitted via the VPN tunnel before negotiating a new key. A setting of 0 disables the rekey data count.
Advanced	Click **Advanced** to configure detailed VPN client tunnel termination settings.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

VPN Client Termination IP pool summary

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Configure IP Address Pool** link to open the screen in Figure 80. Use this screen to manage the list of ranges of IP addresses to assign to the Contivity VPN clients.

Figure 80 VPN Client Termination IP pool summary

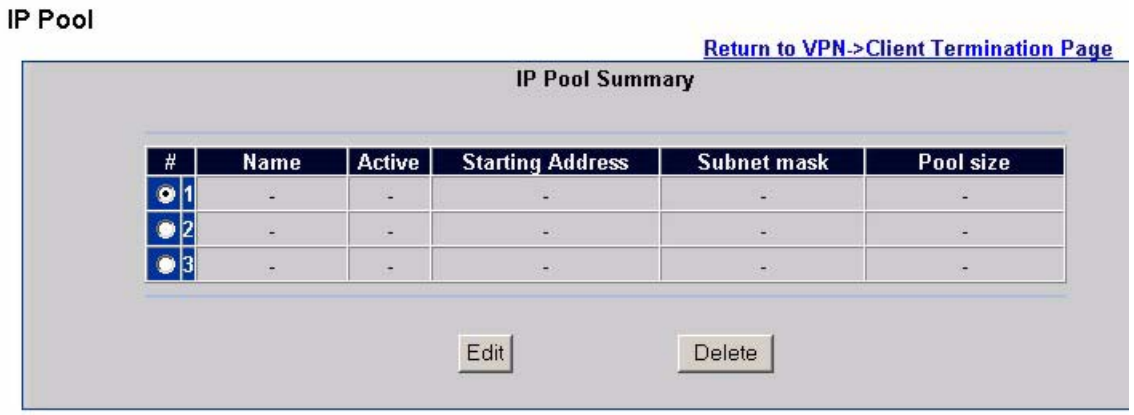

IP Pool
Return to VPN->Client Termination Page
IP Pool Summary
Name Active Starting Address Subnet mask Pool size
1 - - - - -
2 - - - - -
3 - - - - -
Edit
Delete

Table 63 describes the fields in Figure 80.

Table 63 VPN Client Termination IP pool summary

Label	Description
Return to ->Client Termination Page	Click this link to return to the screen used to configure the general settings for use with all of the Contivity VPN Client tunnels.
#	These numbers are an incremental value. The position of the IP address pool in the list does not matter.
Name	This field displays the label that you configure for the IP address pool.
Active	This field displays whether or not the IP address pool is turned on.
Starting Address	This field displays the first IP address in the IP address pool.
Subnet mask	This field displays the subnet mask that you specified to define the IP address pool.
Pool size	This field displays how many IP addresses you set the Business Secure Router to give out from the pool created by the starting address and subnet mask.
Edit	Click the radio button next to an IP address pool entry and click **Edit** to open the screen where you can configure the entry's settings.
Delete	Click the radio button next to an IP address pool entry and click **Delete** to remove it.

VPN Client Termination IP pool edit

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Configure IP Address Pool** link to open the **VPN Client Termination IP Pool Summary** screen. Click the radio button next to an IP address pool entry and click **Edit** to open the following screen where you can configure the entry's settings. Use this screen to configure a range of IP addresses to assign to the Contivity VPN clients.

Figure 81 VPN Client Termination IP pool edit

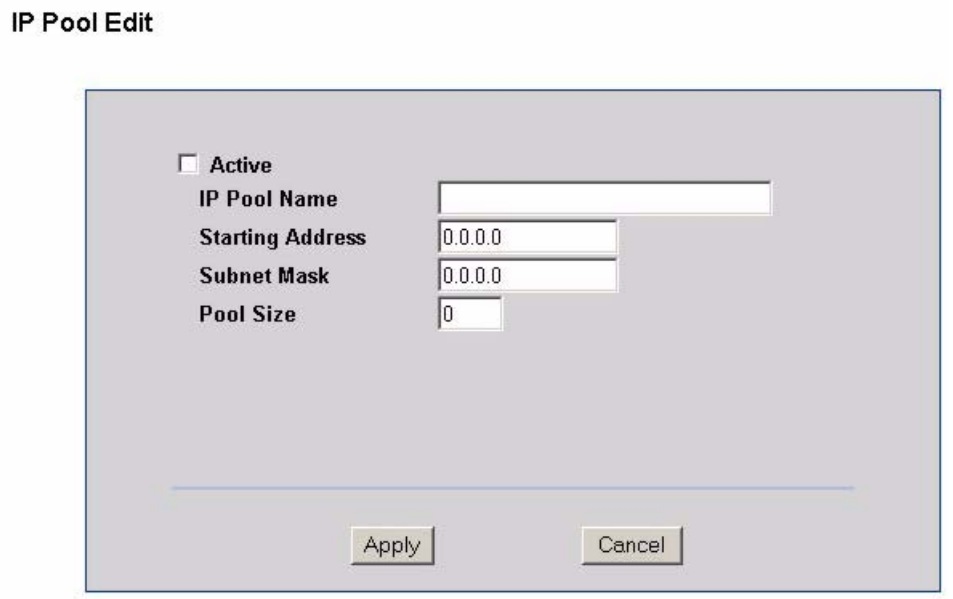


Table 64 describes the fields in Figure 81.

Table 64 VPN Client Termination IP pool edit

Label	Description
Active	Turn on the IP pool if you want the Business Secure Router to use it in assigning IP addresses to the Contivity VPN clients.
IP Pool Name	Specify a label for the IP address pool.
Starting Address	Specify the first of the IP addresses in the IP address pool.
Subnet Mask	Specify a subnet mask to define the IP address pool.

Table 64 VPN Client Termination IP pool edit

Label	Description
Pool Size	Specify how many IP addresses the Business Secure Router is to give out from the pool created by the starting address and subnet mask. 256 is the maximum.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to return to the **IP Pool Summary** screen without saving your changes.

VPN Client Termination advanced

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Advanced** button to open the following screen. Use this screen to configure detailed settings for use with all of the Contivity VPN Client tunnels.

Figure 82 VPN Client Termination advanced

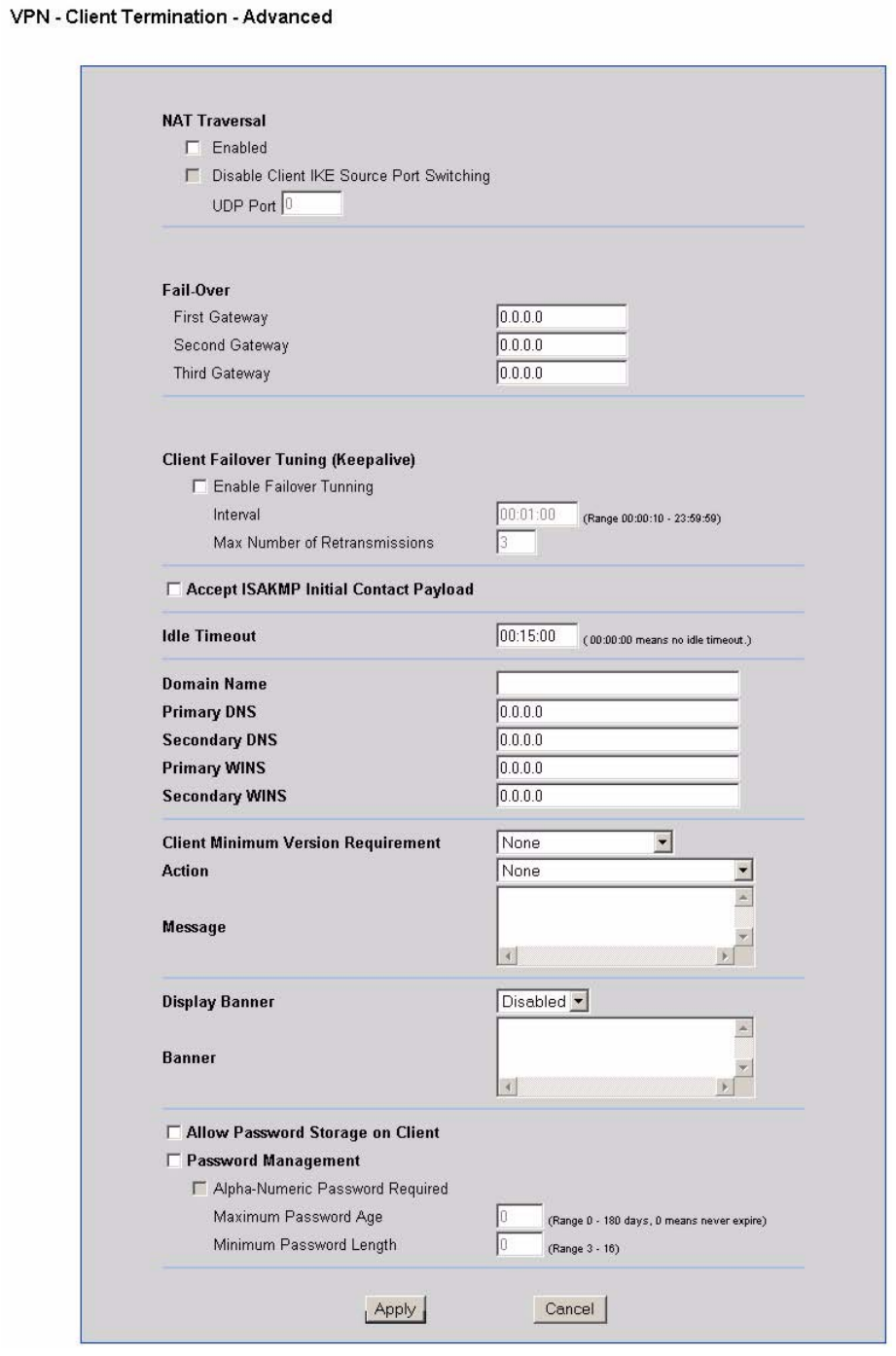


Table 65 describes the fields in Figure 82.

Table 65 VPN Client Termination advanced

Label	Description
NAT Traversal	Select **Enabled** in order to Use NAT traversal when there is a NAT router between the Business Secure Router and the Contivity VPN clients. The Contivity VPN clients must also have NAT traversal enabled. You also need to specify the UDP port that is used for the VPN traffic.
Disable Client IKE Source Port Switching	With client IKE source port switching, if the Business Secure Router detects that traffic is going through NAT, it asks the client to use a UDP port higher than the standard of 500 (such as port 1023). Turn off client source port switching if the NAT router requires IKE to use port 500.
UDP Port	Specifies the UDP port to use for the VPN traffic. In order for a Contivity VPN client behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward this UDP port to the VPN Contivity client behind the NAT router.
Fail-Over	The fail-over feature allows a Contivity VPN client to establish a VPN connection to a backup VPN switch when the Business Secure Router is not accessible. The VPN fail-over feature must also be set up in the Contivity VPN clients.
First Gateway Second Gateway Third Gateway	Enter the IP addresses of the backup VPN switches. When the Business Secure Router is unreachable or fails to respond to IKE negotiation, the Contivity VPN client tries to establish a VPN connection to a backup VPN switch.
Enable Failover Tuning	Enable the VPN fail-over feature to have the Business Secure Router keep sending keep-alive packets to the Contivity VPN clients in order to check the connection and keep the connection alive.
Interval	Specifies how long the VPN Contivity client waits between VPN connection checks.
Max Number of Retransmissions	Specifies the maximum number of retransmissions (0~255) of the keep-alive packets. This is how many times the VPN Contivity client can resend the keep-alive packet to the Business Secure Router to check the connection before attempting to use the first fail-over gateway.

Table 65 VPN Client Termination advanced

Label	Description
Accept ISAKMP Initial Contact Payload	The Business Secure Router can accept the INITIAL-CONTACT status messages to inform it that the Contivity VPN client is establishing a first SA. The Business Secure Router then deletes the existing SAs because it assumes that the sending Contivity VPN client has restarted and no longer has access to any of the existing SAs.
Idle Timeout	Specifies how long the Contivity VPN client connection can go without traffic before the Business Secure Router terminates the session. The Business Secure Router does not time out idle connections when this field is set to 00:00:00.
Domain Name	Specifies the domain name that is used while the VPN tunnel is connected.
Primary DNS Secondary DNS	Specifies the first and second DNS server IP addresses to assign to the Contivity VPN clients.
Primary WINS Secondary WINS	Specifies the first and second WINS server IP addresses to assign to the Contivity VPN clients.
Client Minimum Version Requirement	Selects the lowest version of Contivity VPN client software that you require the clients to use.
Action	Specifies what the Business Secure Router does when it detects a noncompliant version of Contivity VPN client software. Select **None** to allow the VPN tunnel without displaying any messages to tell the user where to download the required version of the Contivity VPN client software. Select **Send Message** to allow the VPN tunnel, but display a message to tell the user where to download the required version of the Contivity VPN client software. Select **Send Message and Force Logoff** to disconnect the VPN tunnel and display a message to tell the user where to download the required version of the Contivity VPN client software.
Message	Enter a message that tells where to download the required version of the Contivity VPN client software. Use from 1 to 255 ASCII characters.
Display Banner	Select **Enabled** to have the Business Secure Router show the Contivity VPN client users a message across the top of the screen after they log on.
Banner	Enter the message (such as the name of your company) that you want to show at the top of the Contivity VPN client users' screens after they log on. Use from 1 to 255 ASCII characters.
Allow Password Storage on Client	Use this to let the Contivity VPN clients save their logon passwords instead of always having to enter them manually.

Table 65 VPN Client Termination advanced

Label	Description
Password Management	You can have the Business Secure Router use some password requirements to enhance security.
Alpha-Numeric Password Required	Use this to have the Business Secure Router require the Contivity VPN client passwords to have both numbers and letters.
Maximum Password Age	Enter the maximum number of days that a Contivity VPN client can use a password before it has to be changed. 0 means that a password never expires.
Minimum Password Length	Enter the minimum number of characters that can be used for a Contivity VPN client password.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 14
Certificates

This chapter gives background information about public-key certificates and explains how to use them.

Certificates overview

The Business Secure Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the Business Secure Router to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Business Secure Router uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that is sent after establishing a connection. The method used to secure the data that is sent through an established connection depends on the type of connection. For example, a VPN tunnel can use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Business Secure Router does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Business Secure Router can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures, and policies that handles keys is called PKI (public-key infrastructure).

Advantages of certificates

Certificates offer the following benefits:

- The Business Secure Router only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure because you can freely distribute public keys and you never need to transmit private keys.

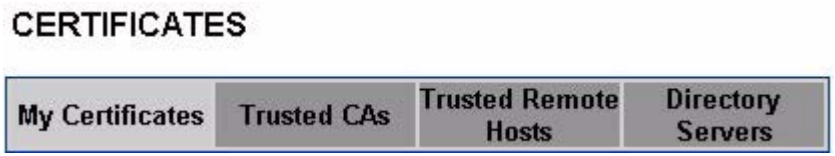
Self-signed certificates

Until public-key infrastructure becomes more mature, it is not available in some areas. You can have the Business Secure Router act as a certification authority and sign its own certificates.

Configuration summary

This section summarizes how to manage certificates on the Business Secure Router.

Figure 83 Certificate configuration overview



Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the Business Secure Routers' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the Business Secure Router.

Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

My Certificates

Click **CERTIFICATES**, **My Certificates** to open the Business Secure Router's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray, as shown in Figure 84.

Figure 84 My Certificates

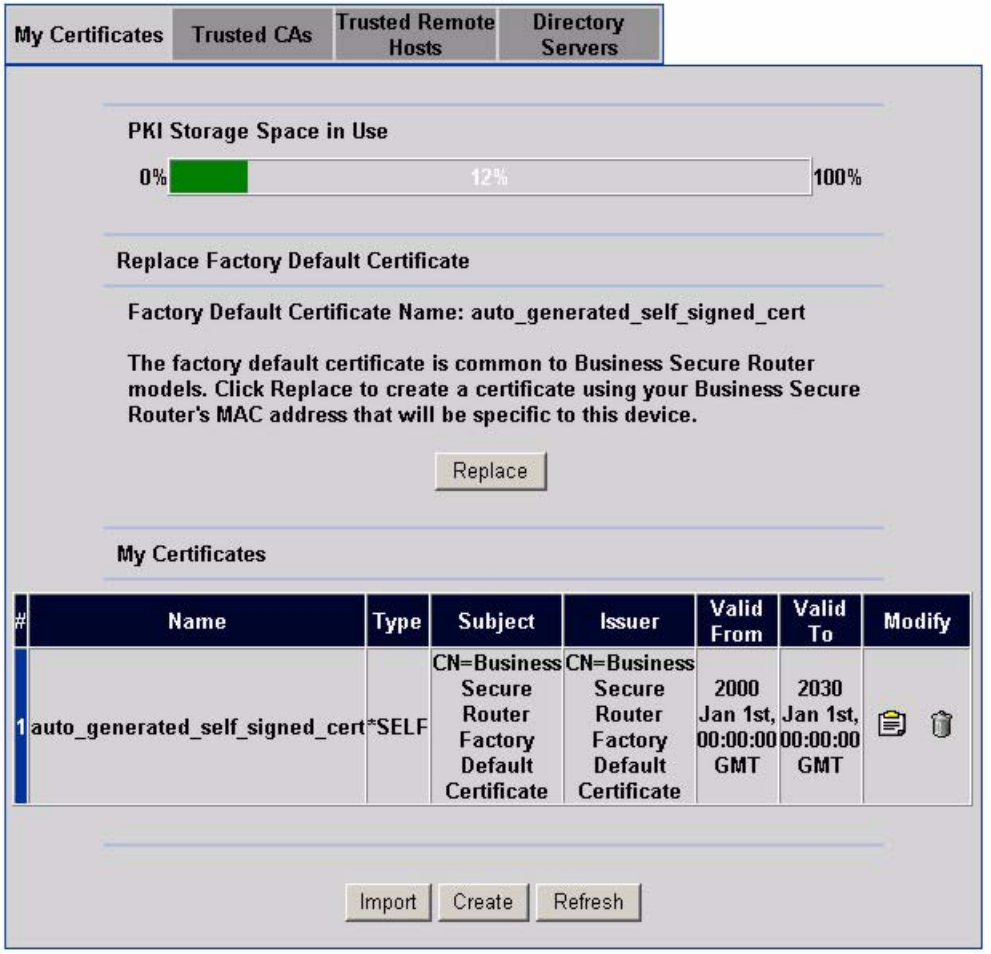

My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
12%
100%
Replace Factory Default Certificate
Factory Default Certificate Name: auto_generated_self_signed_cert
The factory default certificate is common to Business Secure Router models. Click Replace to create a certificate using your Business Secure Router's MAC address that will be specific to this device.
Replace
My Certificates
Name Type Subject Issuer Valid From Valid To Modify
1 auto_generated_self_signed_cert *SELF CN=Business Secure Router Factory Default Certificate CN=Business Secure Router Factory Default Certificate 2000 Jan 1st, 00:00:00 GMT 2030 Jan 1st, 00:00:00 GMT
Import
Create
Refresh

Table 66 describes the labels in Figure 84.

Table 66 My Certificates

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Business Secure Router's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the Business Secure Router has the factory default certificate. The factory default certificate is common to all Business Secure Routers that use certificates. Nortel recommends that you use this button to replace the factory default certificate with one that uses your Business Secure Router's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. Nortel recommends that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the Business Secure Router uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). Nortel recommends that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization, or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 66 My Certificates

Label	Description
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays, asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features are configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, or SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the Business Secure Router.
Create	Click **Create** to go to the screen where you can have the Business Secure Router generate a certificate or a certification request.
Refresh	Click **Refresh** to display the current validity status of the certificates.

Certificate file formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that can be encrypted. The Business Secure Router currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Importing a certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions on the screen shown in Figure 85 to save an existing certificate to the Business Secure Router.

Note: 1. You can only import a certificate that matches a corresponding certification request generated by the Business Secure Router.

Note: 2. The certificate you import replaces the corresponding request in the **My Certificates** screen.

Note: 3. You must remove any spaces from the certificate's filename before you can import it.

Figure 85 My Certificate Import

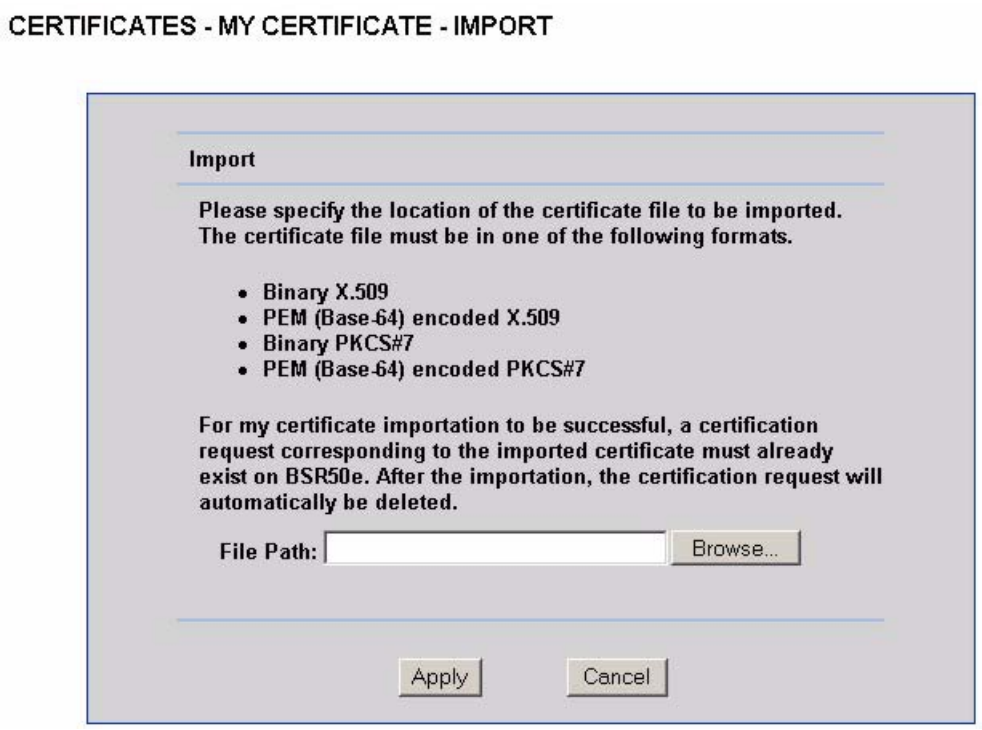

CERTIFICATES - MY CERTIFICATE - IMPORT
Import
Please specify the location of the certificate file to be imported.
The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on BSR50e. After the importation, the certification request will automatically be deleted.
File Path:
Browse...
Apply
Cancel

Table 67 describes the labels in Figure 85.

Table 67 My Certificate Import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate to the Business Secure Router.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

Creating a certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the Business Secure Router create a self-signed certificate, enroll a certificate with a certification authority, or generate a certification request. For more information, see Figure 86.

Figure 86 My Certificate create

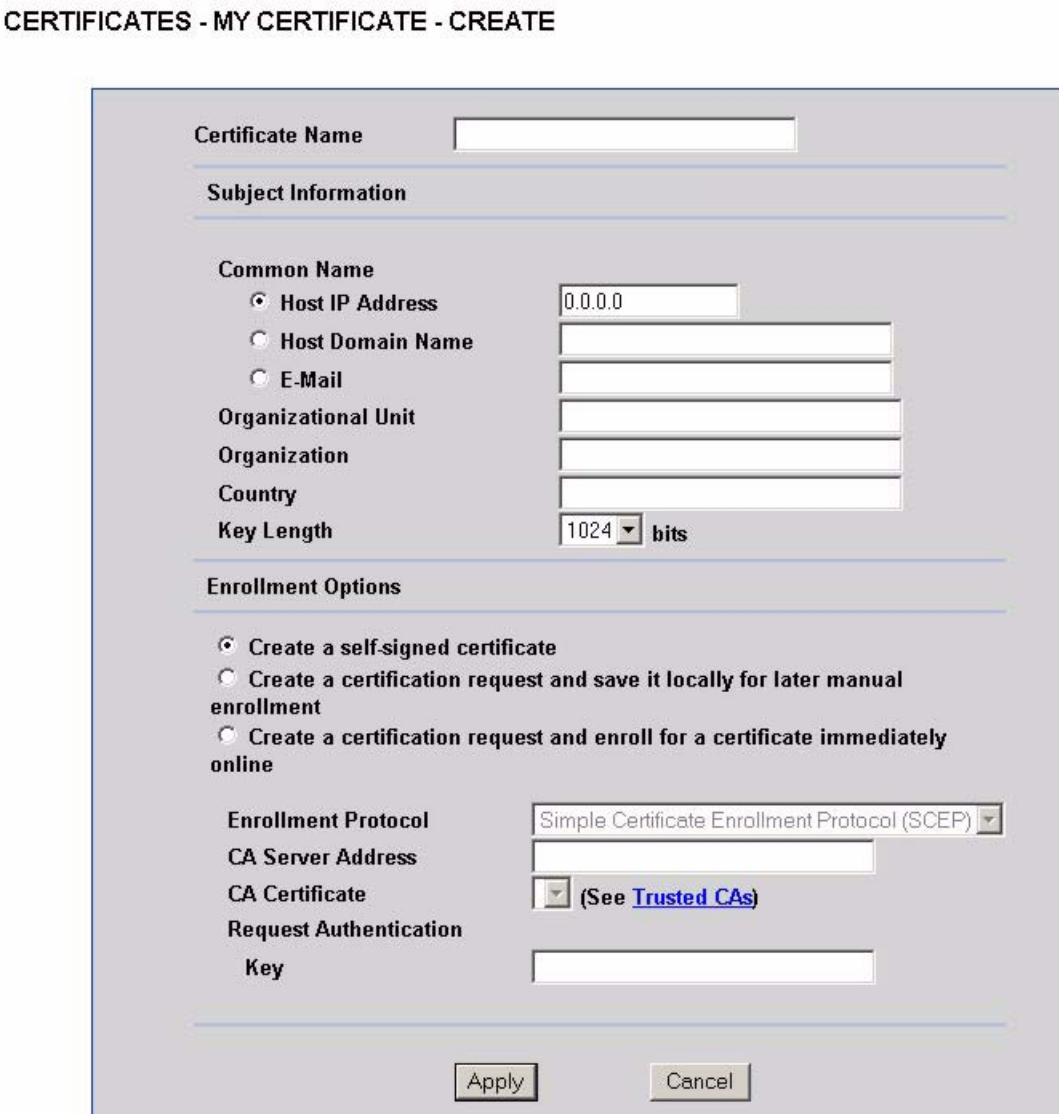


Table 68 describes the labels in the Figure 86.

Table 68 My Certificate create

Label	Description
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority can add fields (such as a serial number) to the subject information when it issues a certificate. Nortel recommends that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name, or e-mail address. Type the IP address (in dotted decimal notation), domain name, or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You can use any character, including spaces, but the Business Secure Router drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You can use any character, including spaces, but the Business Secure Router drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You can use any character, including spaces, but the Business Secure Router drops trailing spaces.
Key Length	Select a number from the drop-down list to determine how many bits are used for the key (512 to 2 048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the Business Secure Router generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.

Table 68 My Certificate create

Label	Description
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the Business Secure Router generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see "My Certificate details" on page 272) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the Business Secure Router generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list and enter the certification authority's server address (or URL). You also need to fill in the **Reference Number** and **Key** if the certification authority requires it.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the Business Secure Router's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority can require you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.

Table 68 My Certificate create

Label	Description
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the Business Secure Router is generating the self-signed certificate or certification request.

After the Business Secure Router successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the Business Secure Router enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Business Secure Router to enroll a certificate online.

My Certificate details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 84). Click the details icon to open the **My Certificate Details** screen. You can use this screen (see Figure 87) to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the Business Secure Router uses to sign the trusted remote host certificates that you import to the Business Secure Router.

Figure 87 My Certificate details

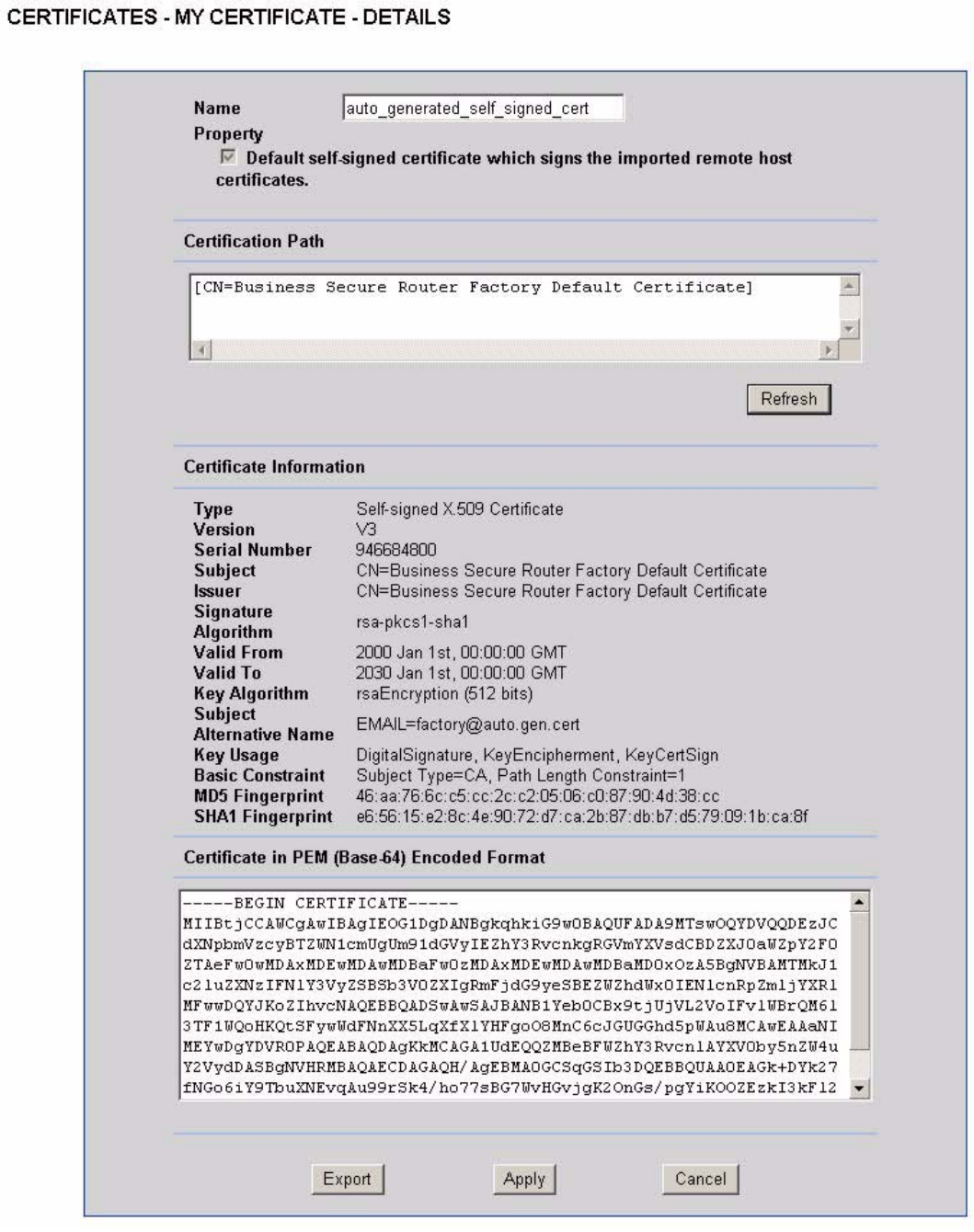


Table 69 describes the labels in Figure 87.

Table 69 My Certificate details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You can use any character (not including spaces).
Property Default self-signed certificate that signs the imported remote host certificates.	Select this check box to have the Business Secure Router use this certificate to sign the trusted remote host certificates that you import to the Business Secure Router. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it can be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Business Secure Router does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Business Secure Router.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) or Country (C).

Table 69 My Certificate details

Label	Description
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization or Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The Business Secure Router uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities can use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Business Secure Router uses RSA encryption) and the length of the key set in bits (1 024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the SHA1 algorithm.

Table 69 My Certificate details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's Web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk, for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen displays, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes to the Business Secure Router. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

Trusted CAs

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen, shown in Figure 88. This screen displays a summary list of certificates of the certification authorities that you have set the Business Secure Router to accept as trusted. The Business Secure Router accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 88 Trusted CAs

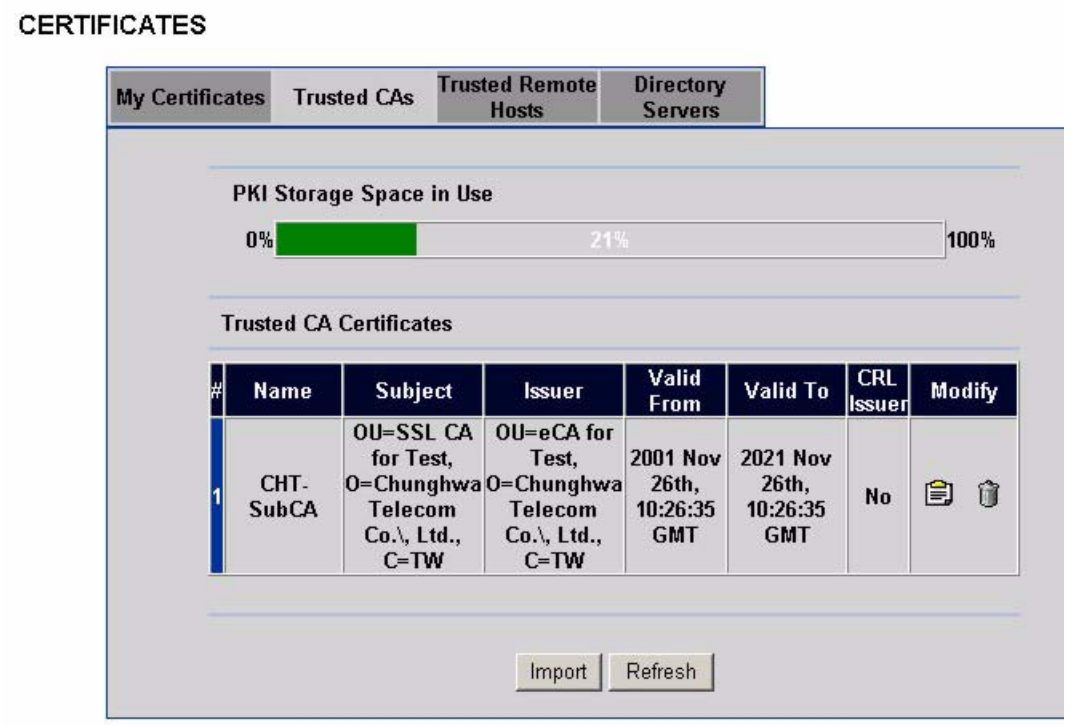


Table 70 describes the labels in Figure 88.

Table 70 Trusted CAs

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Business Secure Router's PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) or C (Country). Nortel recommends that each certificate have unique subject information.

Table 70 Trusted CAs

Label	Description
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization, or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the Business Secure Router check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window appears asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Business Secure Router.
Refresh	Click this button to display the current validity status of the certificates.

Importing a Trusted CA's certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen, shown in Figure 89. Follow the instructions in this screen to save a trusted certification authority's certificate to the Business Secure Router.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 89 Trusted CA import

CERTIFICATES - TRUSTED CA - IMPORT
Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Apply
Cancel

Table 71 describes the labels in Figure 89.

Table 71 Trusted CA import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.

Table 71 Trusted CA import

Label	Description
Apply	Click **Apply** to save the certificate on the Business Secure Router.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

Trusted CA Certificate details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen, shown in Figure 90. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name, and set whether or not you want the Business Secure Router to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 90 Trusted CA details

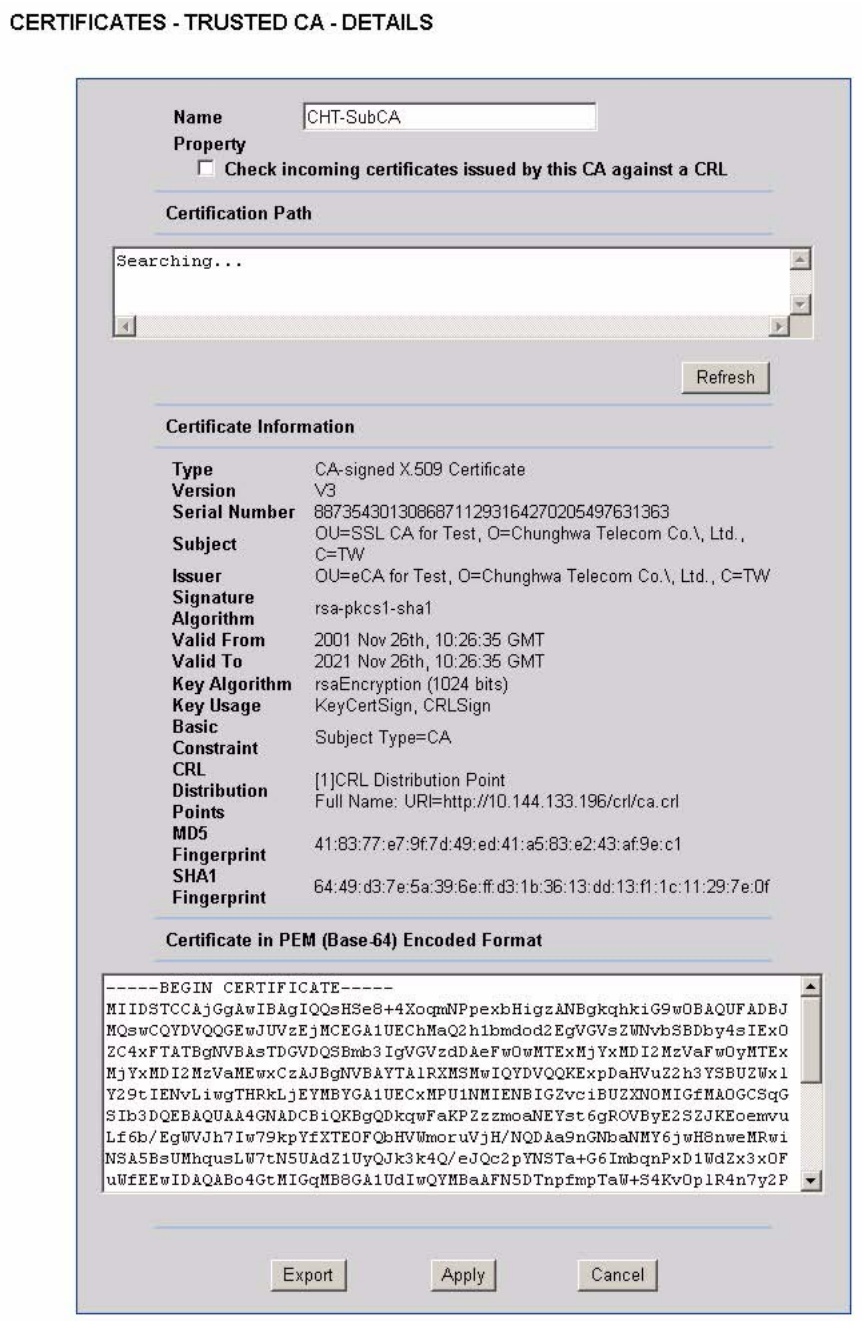


Table 72 describes the labels in Figure 90.

Table 72 Trusted CA details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You can use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the Business Secure Router check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the Business Secure Router not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it can be the only certification authority in the list (along with the end entity's own certificate). The Business Secure Router does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), or Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization or Country. With self-signed certificates, this is the same information as in the **Subject Name** field.

Table 72 Trusted CA details

Label	Description
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities can use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Business Secure Router uses RSA encryption) and the length of the key set in bits (1 024-bits, for example).
Subject Alternative Name	This (optional) field displays the certificate's owner's IP address (IP), domain name (DNS), or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone, for example) that this is actually a valid certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone, for example) that this is actually a valid certificate.

Table 72 Trusted CA details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen displays, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes to the Business Secure Router. You can only apply changes to the name, set the Business Secure Router to check the CRL issued by the certification authority before trusting a certificate issued, or both.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

Trusted remote hosts

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen (see Figure 91). This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen because the Business Secure Router automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 91 Trusted remote hosts

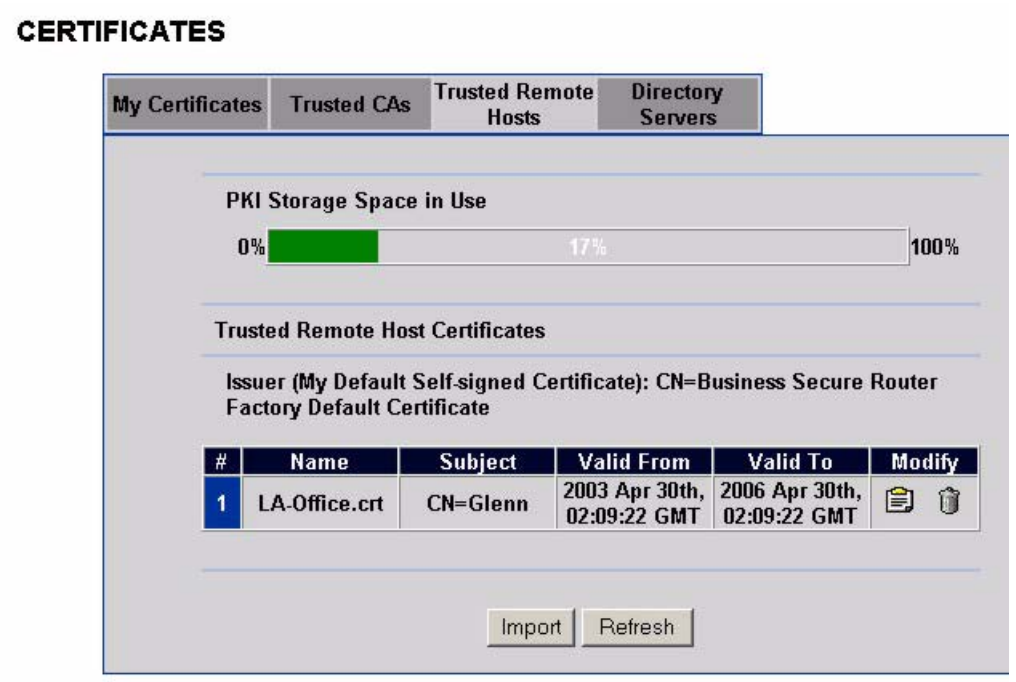


Table 73 describes the labels in Figure 91.

Table 73 Trusted Remote Hosts

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Business Secure Router's PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the Business Secure Router that the Business Secure Router uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.

Table 73 Trusted Remote Hosts

Label	Description
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company), or C (Country). Nortel recommends that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Import	Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the Business Secure Router.
Refresh	Click this button to display the current validity status of the certificates.

Verifying a certificate of a trusted remote host

Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

Trusted remote host certificate fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

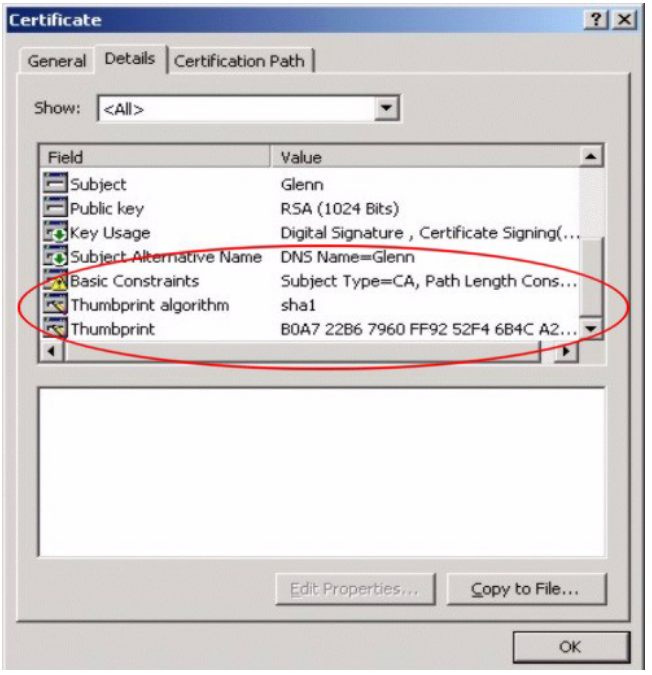
1 Browse to where you have the remote host's certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 92 Remote host certificates

3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 93 Certificate details



Verify (over the phone, for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

Importing a certificate of a trusted remote host

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the Business Secure Router, see Figure 94.

Note: The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its file name before you can import it.

Figure 94 Trusted remote host import

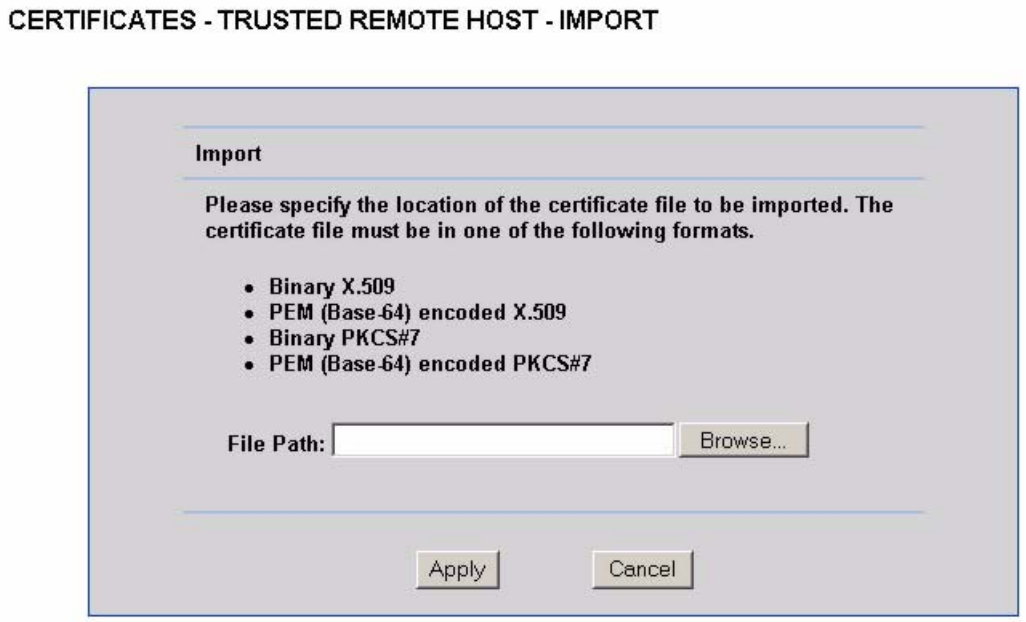

CERTIFICATES - TRUSTED REMOTE HOST - IMPORT
Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Apply
Cancel

Table 74 describes the labels in Figure 94.

Table 74 Trusted remote host import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the Business Secure Router.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

Trusted remote host certificate details

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and change the certificate's name.

Figure 95 Trusted remote host details

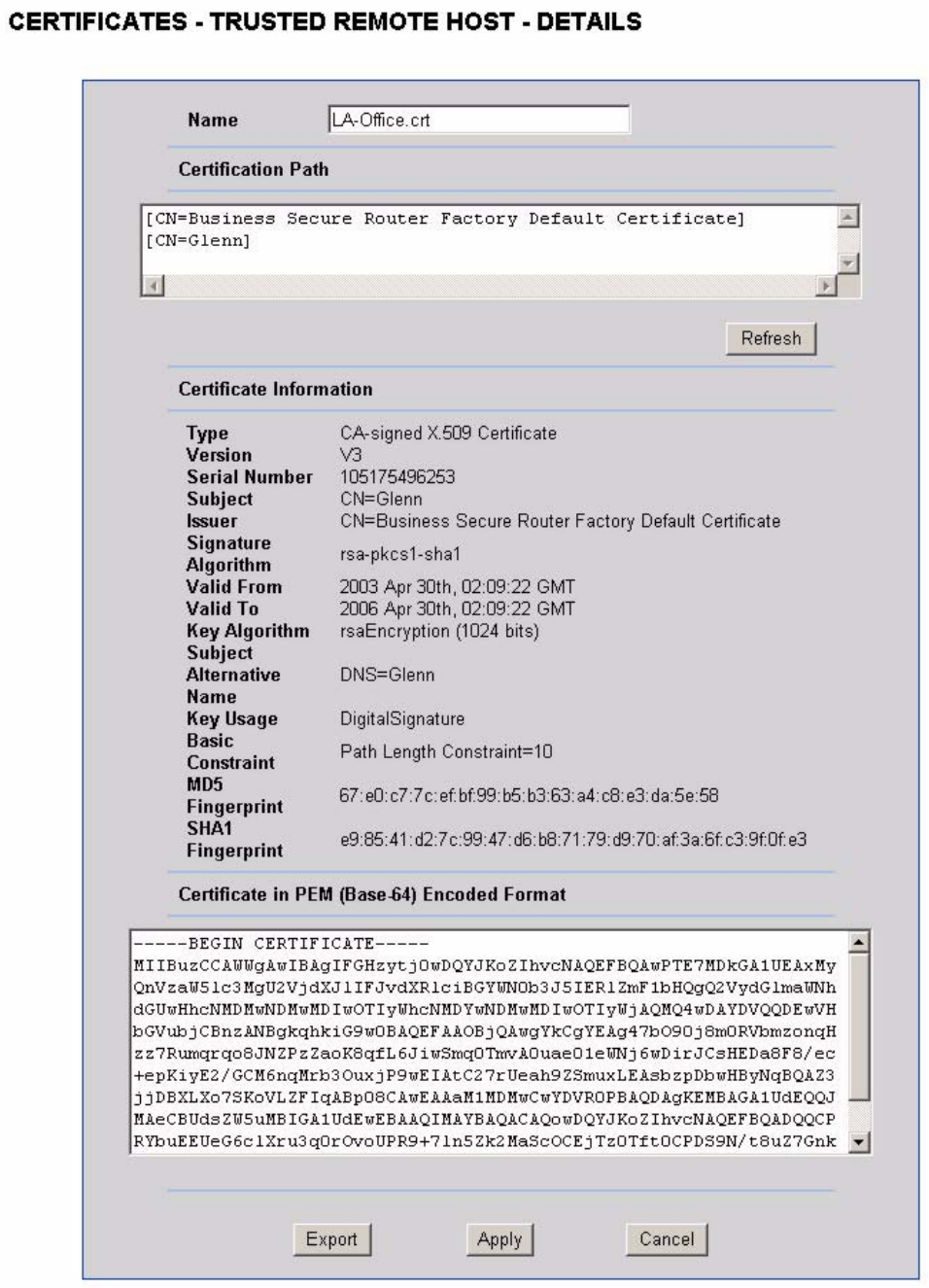


Table 75 describes the labels in Figure 95.

Table 75 Trusted remote host details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You can use any character (not including spaces).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the Business Secure Router uses to sign remote host certificates. Since the Business Secure Router considers its own self-signed certificate to be a certification authority, the chain of certificates is complete and the Business Secure Router trusts the certificate.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The Business Secure Router is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), or Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the Business Secure Router that the Business Secure Router uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the Business Secure Router used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.

Table 75 Trusted remote host details

Label	Description
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Business Secure Router uses RSA encryption) and the length of the key set in bits (1 024-bits, for example).
Subject Alternative Name	This (optional) field displays the certificate owner's IP address (IP), domain name (DNS), or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, DigitalSignature means that the key can be used to sign certificates and KeyEncipherment means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and Path Length Constraint=1 means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the Business Secure Router has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See "Verifying a certificate of a trusted remote host" on page 286 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Business Secure Router calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the Business Secure Router has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See "Verifying a certificate of a trusted remote host" on page 286 for how to verify a remote host's certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen displays. Browse to the location that you want to use and click **Save**.

Table 75 Trusted remote host details

Label	Description
Apply	Click **Apply** to save your changes to the Business Secure Router. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

Directory servers

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen (Figure 96). This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the Business Secure Router. If you decide to have the Business Secure Router check incoming certificates against the issuing certification authority's list of revoked certificates, the Business Secure Router first checks the servers listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the Business Secure Router checks the servers listed here.

Figure 96 Directory servers

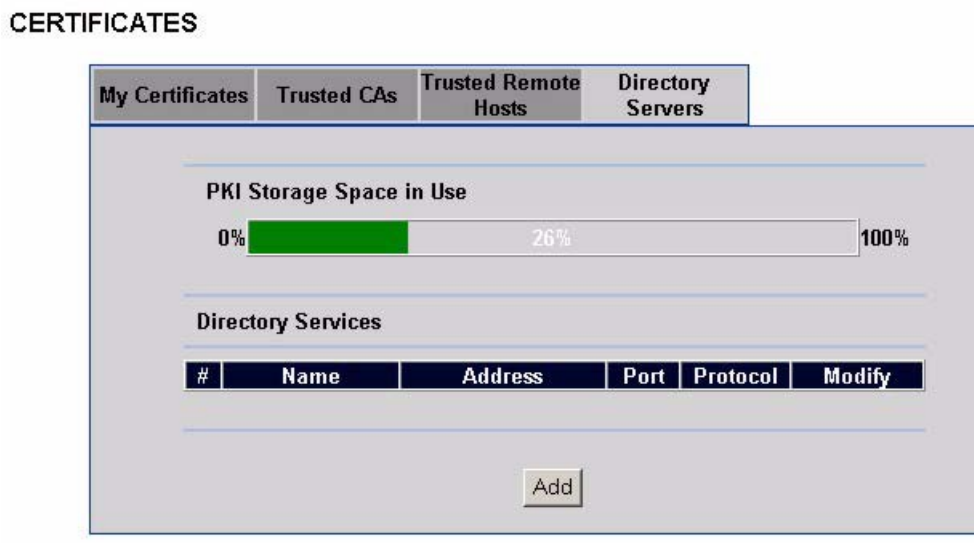


Table 76 describes the labels in Figure 96.

Table 76 Directory Servers

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Business Secure Router's PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Add	Click **Add** to open a screen where you can configure information about a directory server so that the Business Secure Router can access it.

Add or edit a directory server

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to display the screen shown in Figure 97. Use this screen to configure information about a directory server that the Business Secure Router can access.

Figure 97 Directory server add

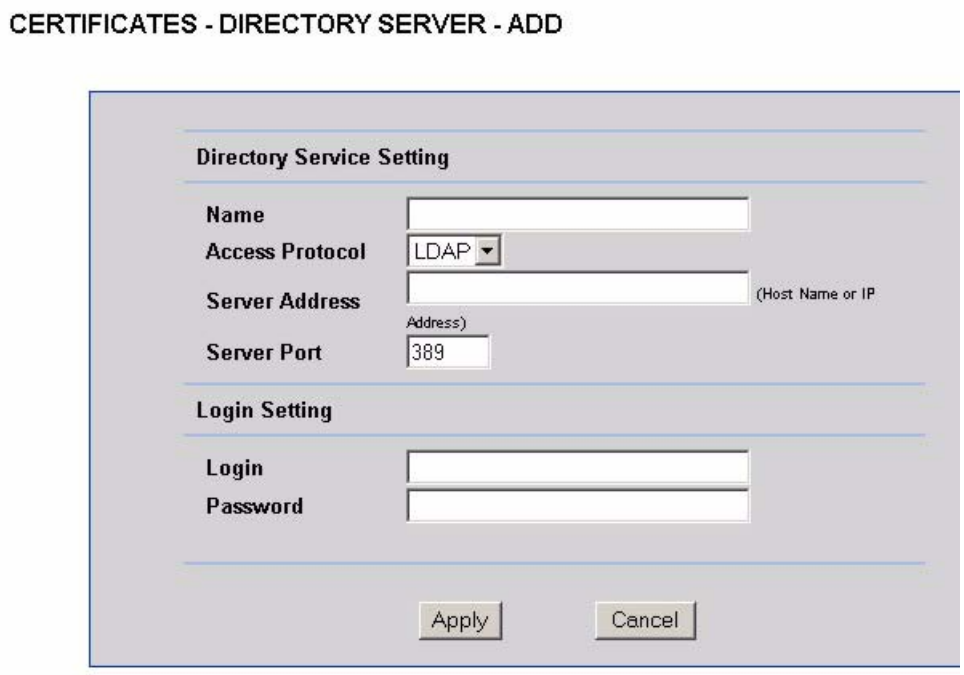


Table 77 describes the labels in Figure 97.

Table 77 Directory server add

Label	Description
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories certificates and lists of revoked certificates.[1]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.

Table 77 Directory server add

Label	Description
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You can change the server port number if needed, however, you must use the same server port number that the directory server uses. The default server port number for LDAP is 389.
Login Setting	
Login	The Business Secure Router must authenticate itself in order to assess the directory server. Type the logon name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen.

1 At the time of writing, LDAP is the only choice for directory server access protocol.

Chapter 15
Bandwidth management

This chapter describes the functions and configuration of bandwidth management.

Bandwidth management overview

With bandwidth management, you can allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Business Secure Router forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- Which traffic must have guaranteed delivery?
- How much bandwidth is allotted to guarantee delivery?

With bandwidth management, you can configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1 024 kb/s (or less) if the broadband device connected to the WAN port has an upstream speed of 1 024 kb/s.

Bandwidth classes and filters

Use bandwidth subclasses to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth subclass based on a specific application or subnet. Use the **Class Setup** tab (see "Bandwidth Manager Class Configuration" on page 303) to set up a bandwidth class name, bandwidth allotment, and filter specifics. Each bandwidth subclass consists of a single filter you can define by editing the subclass.

Unallocated bandwidth, bandwidth that is not controlled by a subclass you specify, is allocated to traffic not controlled by any subclass. View your configured bandwidth subclasses for a given interface in the **Class Setup** tab (see "Configuring class setup" on page 301 for details). The total of the configured bandwidth budgets cannot exceed the configured bandwidth budget for the interface, as specified in "Configuring summary" on page 300.

Proportional bandwidth allocation

With bandwidth management, you can define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

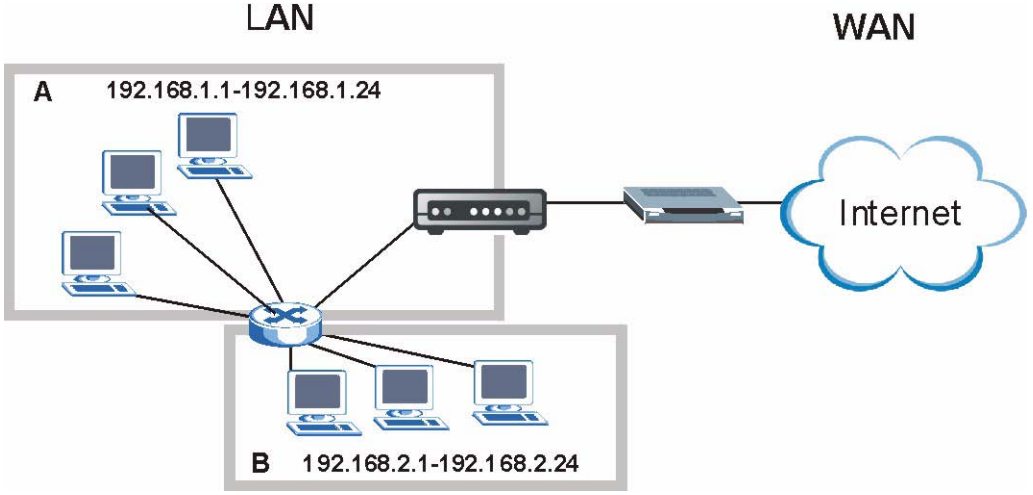
Application based bandwidth management

You can create bandwidth classes based on individual applications (like FTP, H.323, and SIP).

Subnet based bandwidth management

You can create bandwidth classes based on subnets. Figure 98 shows LAN subnets. You can configure one bandwidth class for subnet A and another for subnet B.

Figure 98 Subnet based bandwidth management example



Application and subnet based bandwidth management

You can also create bandwidth classes based on a combination of a subnet and an application. Table 78 shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 78 Application and Subnet based Bandwidth Management Example

Traffic Type	From Subnet A	From Subnet B
FTP	64 Kb/s	64 Kb/s
H.323	64 Kb/s	64 Kb/s
SIP	64 Kb/s	64 Kb/s

Reserving bandwidth for nonbandwidth class traffic

If you want to allow bandwidth for traffic that is not defined in a bandwidth filter, leave some of the interface's bandwidth unbudgeted.

Configuring summary

Click **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 99 Bandwidth Manager: Summary

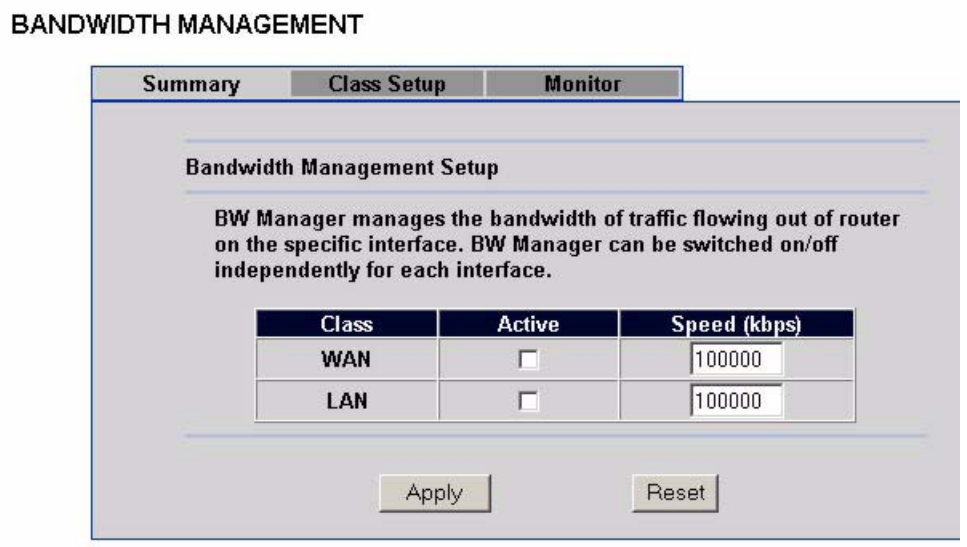


Table 79 describes the labels in Figure 99.

Table 79 Bandwidth Manager: Summary

Label	Description
WAN LAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias cause LAN-to-LAN traffic to pass through the Business Secure Router and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.

Table 79 Bandwidth Manager: Summary

Label	Description
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see "Configuring class setup" on page 301). Nortel recommends that you set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1 000 kb/s (or less) if the broadband device connected to the WAN port has an upstream speed of 1 000 kb/s.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring class setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click **+** to expand the class tree or click **-** to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see "Configuring summary" on page 300 to configure the speed of the interface). Configure subclass layers for the root class.

To add or delete child classes on an interface, click **BW MGMT**, then the **Class Setup** tab. The screen appears as shown in Figure 100.

Figure 100 Bandwidth Manager: Class setup

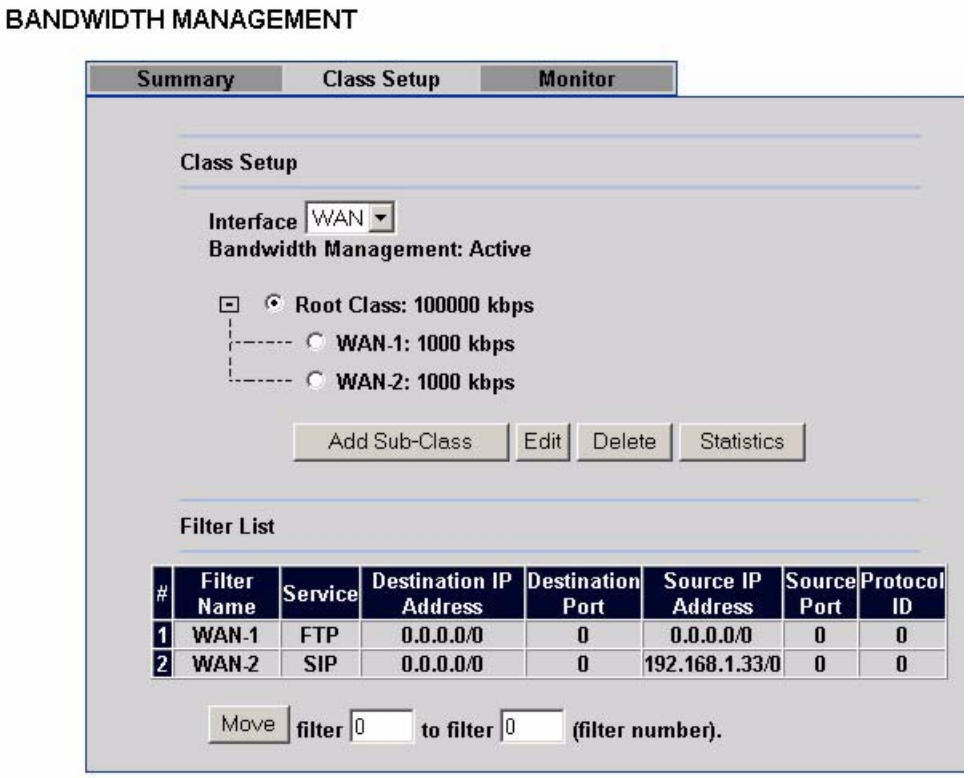


Table 80 describes the labels in Figure 100.

Table 80 Bandwidth Manager: Class Setup

Label	Description
Interface	Select an interface from the drop-down list for which you wish to set up classes.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**).
Add Subclass	Click **Add Sub-class** to add a subclass.
Edit	Click **Edit** to go to a screen where you can configure the selected subclass. You cannot edit the root class.
Delete	Click **Delete** to remove the selected subclass. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

Table 80 Bandwidth Manager: Class Setup

Label	Description
#	This is the number of a filter entry. The ordering of your filters is important, as they are applied in turn. Use the **Move** button to reorder your filters.
Filter Name	This is the **Class Name** that you configured in the **Edit Class** screen.
Service	If you selected a predefined application (FTP, H.323 or SIP), it displays here.
Destination IP Address	This field displays the destination IP address in dotted decimal notation followed by the subnet mask. The IP 0.0.0.0/0 means all.
Destination Port	This field displays the port number of the destination. 0 means all ports.
Source IP Address	This field displays the source IP address in dotted decimal notation followed by the subnet mask. The IP 0.0.0.0/0 means all.
Source Port	This field displays the port number of the source. The 0 means all ports.
Protocol ID	This field displays the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. The 0 means all protocols.
Move	Type the number of a filter entry and the number for where you want to put it. Click **Move** to move the filter to the number that you typed. The ordering of your filters is important, as they are applied in order of their numbering. The filter entry numbers are not static names for the entries. A filter entry's number changes as you move the filter entry up or down in the list. Also, only the existing filter entries are counted, you cannot have any blank filter entries. For example, if you have only three filters and try to move number one to seven, it becomes filter three.

Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure subclasses for that interface.

To add a subclass, click **BW MGMT**, and then the **Class Setup** tab. Click the **Add Sub-Class** button to open the screen shown in Figure 101.

Figure 101 Bandwidth Manager: Edit class

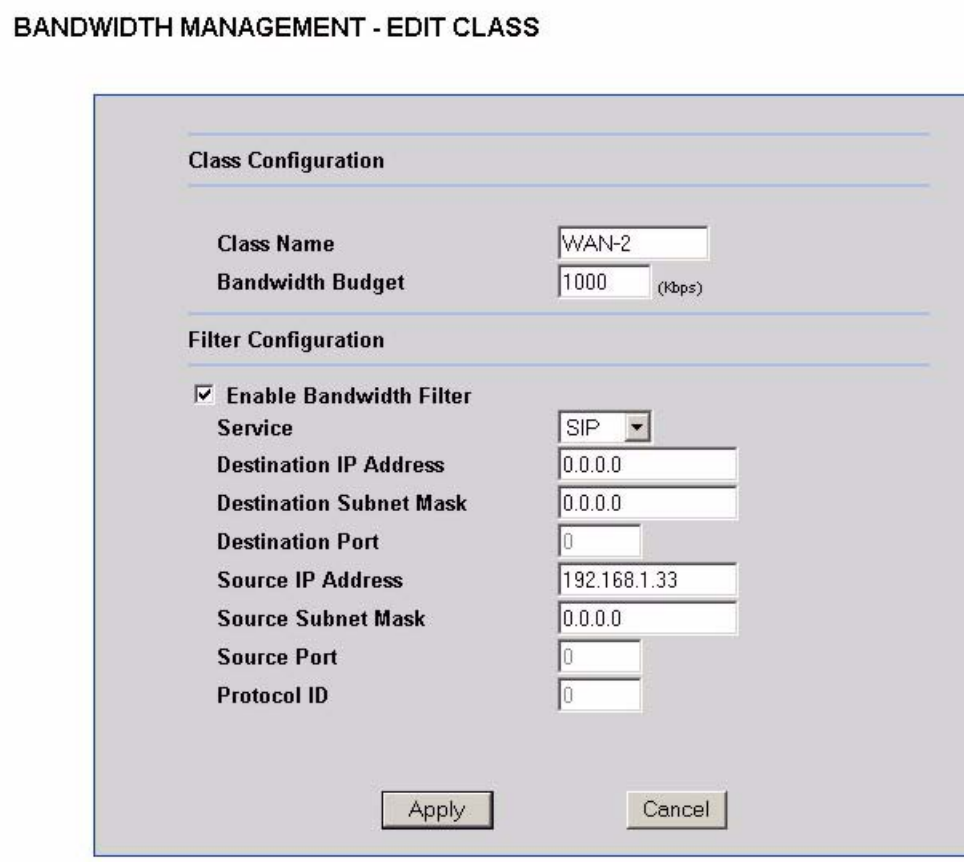


Table 81 describes the labels in Figure 101.

Table 81 Bandwidth Manager: Edit class

Label	Description
Class Configuration	
Class Name	Use the autogenerated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kb/s. The recommendation is a setting between 20 kbps and 20 000 kbps for an individual class. The bandwidth you specify cannot cause the total allocated bandwidths of this and all other subclasses to exceed the bandwidth for the interface.

Table 81 Bandwidth Manager: Edit class

Label	Description
Filter Configuration	
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the Business Secure Router use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields, which are only available when you enter the destination or source IP address).
Service	This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not need to configure the rest of the bandwidth filter fields (other than the **Active** check box). **FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that are not possible by e-mail. Select FTP from the drop-down list to configure the bandwidth filter for FTP traffic. If you select **FTP**, make sure you also turn on the FTP ALG. For more information about ALG, see “ALG” on page 90. **H.323** is a protocol standard used for multimedia communications over networks, for example, NetMeeting. Select H.323 from the drop-down list to configure the bandwidth filter for H.323 traffic. If you select **H.323**, make sure you also turn on the H.323 ALG. For more information about ALG, see “ALG” on page 90. **SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification, and conferencing. The Business Secure Router supports SIP traffic pass through. Select SIP from the drop-down list to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN. If you select **SIP**, make sure you also turn on the SIP ALG. For more information about ALG, see “ALG” on page 90. Select **All** from the drop-down list if you do not want to use a predefined application for the bandwidth class. When you select **All**, you must configure at least one of the following fields (other than the **Subnet Mask** fields, which you only enter if you also enter a corresponding destination or source IP address).
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**.
Destination Port	Enter the port number of the destination. See “Predefined services” on page 188 in Chapter 11 Firewall screens for a table of services and port numbers.

Table 81 Bandwidth Manager: Edit class

Label	Description
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source IP Address**.
Source Port	Enter the port number of the source. See Table 82 for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to exit this screen without saving.

Table 82 Services and port numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Bandwidth management statistics

Use the **Bandwidth Management Statistics** screen to view network performance for the interface (root class) or a specific subclass. Select the root or subclass from the **Class Setup** screen and then click **Statistics** to see how it is performing.

Figure 102 Bandwidth management statistics

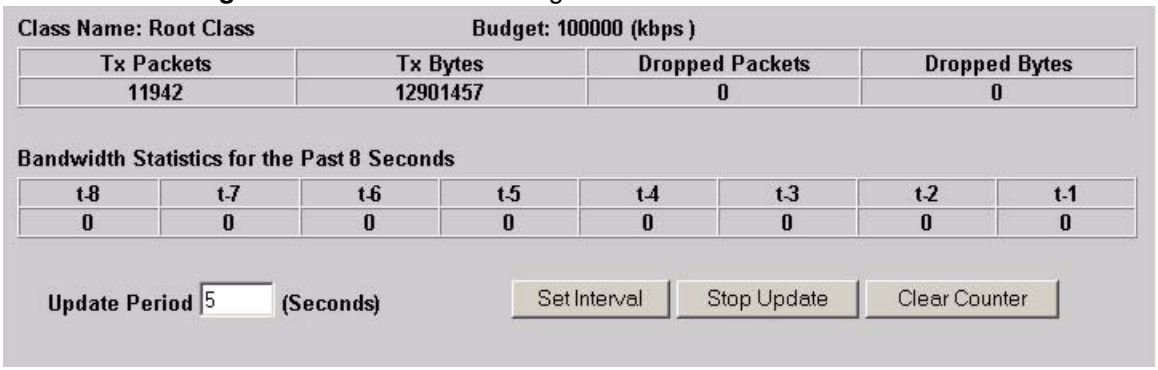


Table 83 describes the labels in Figure 102.

Table 83 Bandwidth management statistics

Label	Description
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in b/s) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (Seconds)	Enter the time interval, in seconds, to define how often the information is refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

Monitor

To view the device's bandwidth usage and allotments, click **BW MGMT**, then the **Monitor** tab. The screen appears as shown in Figure 103.

Figure 103 Bandwidth manager monitor

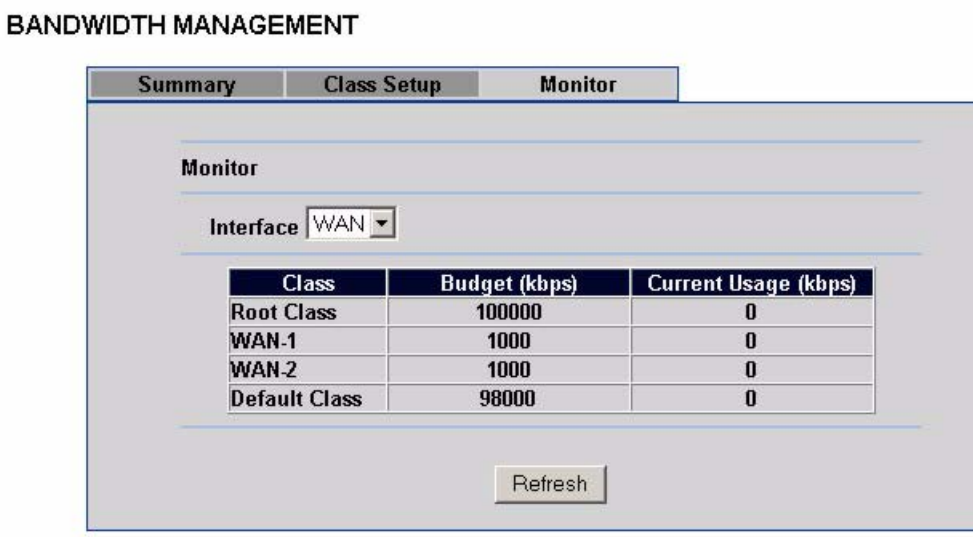


Table 84 describes the labels in Figure 103.

Table 84 Bandwidth manager monitor

Label	Description
Interface	Select an interface from the drop-down list to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Refresh	Click **Refresh** to update the page.

Chapter 16
IEEE 802.1x

IEEE 802.1x overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of users and encryption key management. Authentication can be done using the local user database internal to the Business Secure Router (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where users are the clients and the server is the RADIUS server. The RADIUS server handles the following tasks, among others:

- Authentication

  Determines the identity of the users.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your Business Secure Router acts as a message relay between the user and the network RADIUS server.

Types of RADIUS messages

The following types of RADIUS messages are exchanged between the Business Secure Router and the RADIUS server for user authentication:

- Access-Request

  Sent by the Business Secure Router requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The Business Secure Router sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the Business Secure Router and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the Business Secure Router requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the Business Secure Router and the RADIUS server use a shared secret key, which is a password they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

EAP Authentication overview

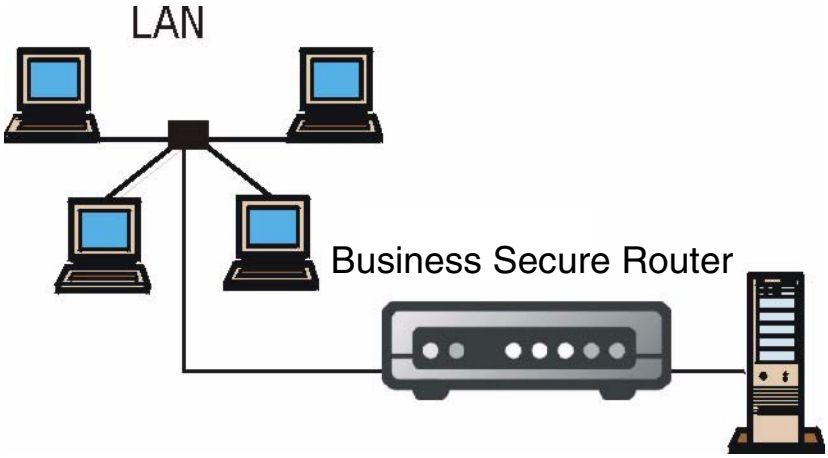
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the Business Secure Router helps a user's computer and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP.

Your Business Secure Router supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database.

Figure 104 shows an overview of authentication when you specify a RADIUS server on your Business Secure Router.

Figure 104 EAP Authentication



The steps below provide a general description of how IEEE 802.1x EAP authentication works.

1. The user sends a start message to the Business Secure Router.
2. The Business Secure Router sends a request identity message to the user for identity information.
3. The user replies with identity information, including username and password.
4. The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the user.

Configuring 802.1X

To change your Business Secure Router's Authentication settings, click **802.1X**. The screen appears, as shown in Figure 105.

Figure 105 802.1X

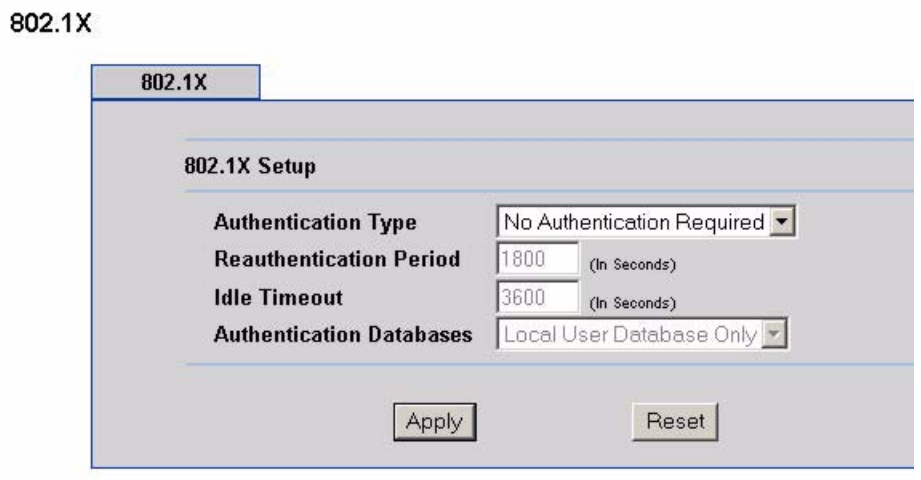


Table 85 describes the labels in Figure 105.

Table 85 802.1X

Label	Description
Authentication Type	Select **Authentication Required**, **No Access** or **No Authentication Required** from the drop-down list. Select **Authentication Required** to authenticate all users before they can access the network. Select **No Authentication Required** to allow all users to access your network without authentication. Select **No Access** to deny all users access to your wired network.
Reauthentication Period	Specifies the time interval between the RADIUS server's authentication checks of users connected to the network. This field is active only when you select **Authentication Required** in the **Authentication Type** field.
Idle Timeout (Seconds)	The Business Secure Router automatically disconnects a user after a period of inactivity. The user needs to enter the username and password again before access is allowed.

Table 85 802.1X

Label	Description
Authentication Databases	The authentication database contains user login information. The local user database is the built-in database on the Business Secure Router. The RADIUS is an external server. Use this drop-down list to select the first database the Business Secure Router will use to authenticate a user. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Business Secure Router just check the built-in user database on the Business Secure Router for a user's username and password. Select **RADIUS Only** to have the Business Secure Router just check the user database on the specified RADIUS server for a user's username and password. Select **Local first, then RADIUS** to have the Business Secure Router first check the user database on the Business Secure Router for a user's username and password. If the user name is not found, the Business Secure Router then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Business Secure Router first check the user database on the specified RADIUS server for a user's username and password. If the Business Secure Router cannot reach the RADIUS server, the Business Secure Router then checks the local user database on the Business Secure Router. When the user name is not found or password does not match in the RADIUS server, the Business Secure Router does not check the local user database and the authentication fails.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 17
Authentication server

The Business Secure Router can use either the local user database internal to the Business Secure Router or an external RADIUS server for an unlimited number of users.

Introduction to Local User database

By storing user profiles locally on the Business Secure Router, your Business Secure Router is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you can authenticate in this way.

Local User database

To see your Business Secure Router's local user list, click **AUTH SERVER**. The **Local User Database** screen appears as shown in Figure 106.

Figure 106 Local User database

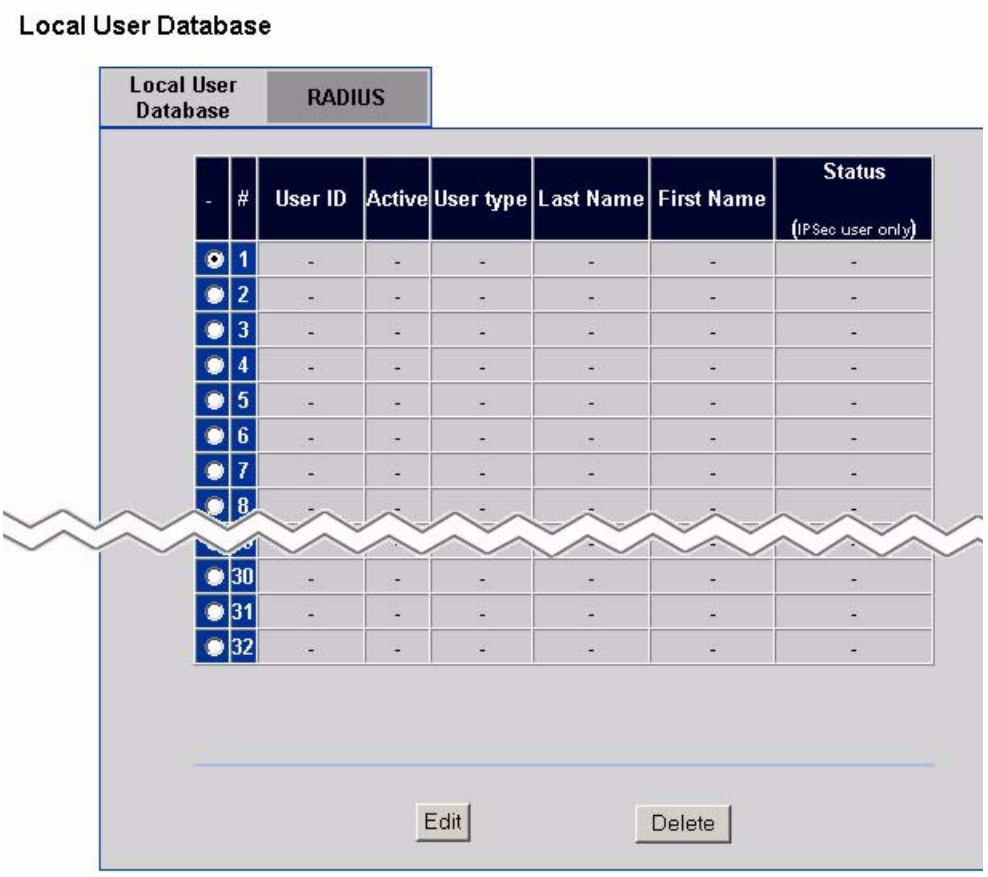


Table 86 describes the labels in Figure 106.

Table 86 Local User database

Label	Description
User ID	This field displays the logon name for the user account.
Active	This field displays **Yes** if the user account is enabled or **No** if it is disabled.
User type	This field displays whether the user account can be used for a IEEE 802.1X or IPSec logon (or both).
Last Name	This field displays the user's last name.
First Name	This field displays the user's first name.

Table 86 Local User database

Label	Description
Status	This field displays the status of IPSec user accounts. A dash appears for all other accounts. **Valid** displays if an IPSec user can use the account to logon. **Expired** displays if an IPSec user can no longer use the account to logon. This happens when you have enabled **Password Management** in the **VPN Client Termination Advanced** screen and the account's password has exceeded the time that you configured as the **Maximum Password Age**.
Edit	Select a user account and click **Edit** to go to the screen where you can configure the account's settings.
Delete	Select a user account and click **Delete** to remove the account.

Edit Local User Database

To change a local user database entry, click **AUTH SERVER**. In the **Local User Database** screen, select an entry's radio button and click the **Edit** button to display the **Local User Database Edit** screen, as shown in Figure 107.

Figure 107 Local User database edit

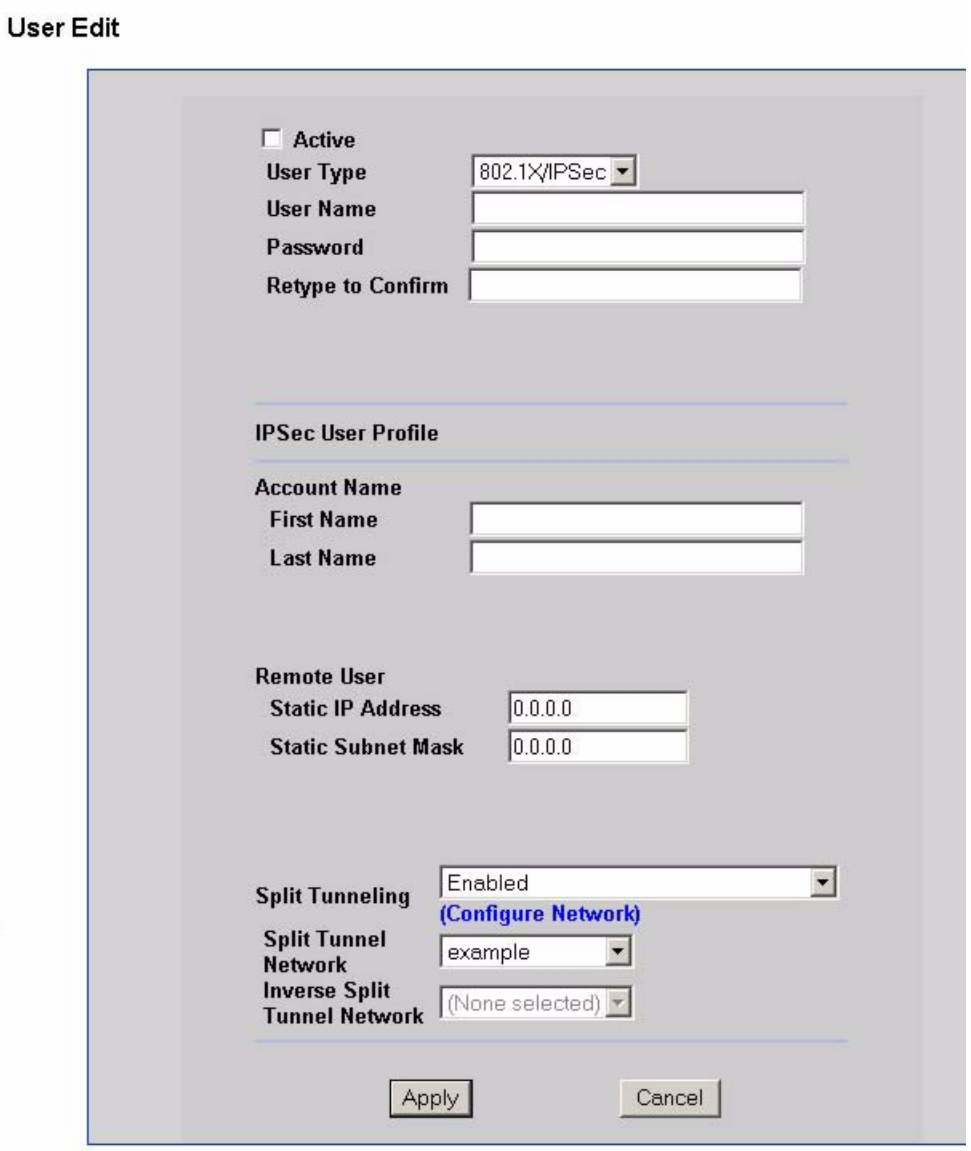


Table 87 describes the labels in Figure 107.

Table 87 Local User database edit

Label	Description
Active	Select this check box to turn on the user account. Clear this check box to turn off the user account.
User Type	Select **802.1X** to set this user account to be used for a IEEE 802.1X logon. Select **IPSec** to set this user account to be used for an IPSec logon. Select **802.1X/IPSec** to set this user account to be used for both IEEE 802.1X and IPSec logons.
User Name	Specify the user ID to be used as the logon name for the user account.
Password	Enter a password up to 31 characters long for this user account. Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
IPSec User Profile	The following fields display when you select **IPSec** or **802.1X/IPSec** in the **User Type** field.
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Static IP Address	Enter the IP address of the remote user in dotted decimal notation.
Static Subnet Mask	Enter the subnet mask of the remote user.
Split Tunneling	Enable or disable split tunneling or inverse split tunneling. Select **Disable** to force all traffic to be encrypted and go through the VPN tunnel. Select **Enabled** to allow traffic not going through the VPN tunnel to go through the WAN interface without being encrypted. This reduces the processing load on the Business Secure Router but is less secure since the Contivity VPN clients' unencrypted sessions make them vulnerable to attacks. Select **Enabled - Inverse** to force traffic not going to the network subnets that you specify to be encrypted and sent through the VPN tunnel. Select **Enable - Inverse (locally connected)** to force traffic not going to directly connected networks, or the network subnets that you specify, to be encrypted and sent through the VPN tunnel.
Configure Network	Click this link to set up the list of networks to use as split or inverse split networks.

Table 87 Local User database edit

Label	Description
Split Tunnel Networks	This field applies when you select **Enabled** in the **Split Tunneling** field. Select the network for which you force traffic to be encrypted and go through the VPN tunnel.
Inverse Split Tunnel Network	This field applies when you select **Enabled - Inverse** or **Enabled - Inverse (locally connected)** in the **Split Tunneling** field. Select the network for which you do not force traffic to be encrypted and go through the VPN tunnel.
Apply	Click **Apply** to save the user account's settings.
Cancel	Click **Cancel** to exit this screen without saving.

Current split networks

In the **Local User Database Edit** screen, click **Configure Network** to display the **Current Split Networks** screen as shown in Figure 108. This screen displays a list of networks that are configured for use with split and inverse split VPN tunnels.

Figure 108 Current split networks

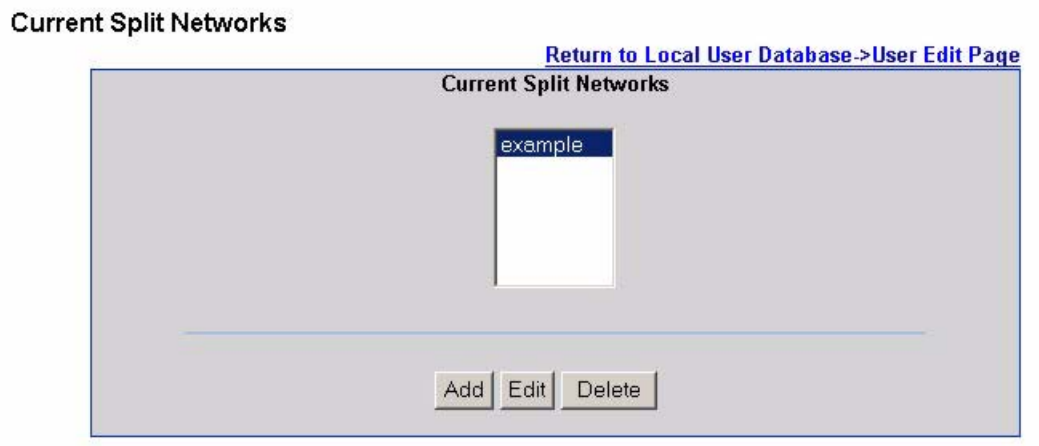


Table 88 describes the labels in Figure 108.

Table 88 Current split networks

Label	Description
Return to Local User Database -> User Edit Page	Click this link to return to the screen where you configure a local user database entry.
Current Split Networks	This is the list of names of split or inverse split networks.
Add	Click **Add** to open another screen where you can specify split or inverse split networks.
Edit	Select the name of a split or inverse split network and click **Edit** to open a screen where you can change the network's settings.
Delete	Select the name of a split or inverse split network and click **Delete** to remove the network entry.

Current split networks edit

In the **Local User Database Edit** screen, click **Configure Network** to display the **Current Split Networks** screen. Click **Add** or select a network and click **Edit** in order to display the **Current Networks Edit** screen. Use this screen shown in Figure 109 to configure a set of subnets to use with split or inverse split VPN tunnels.

Figure 109 Current split networks edit

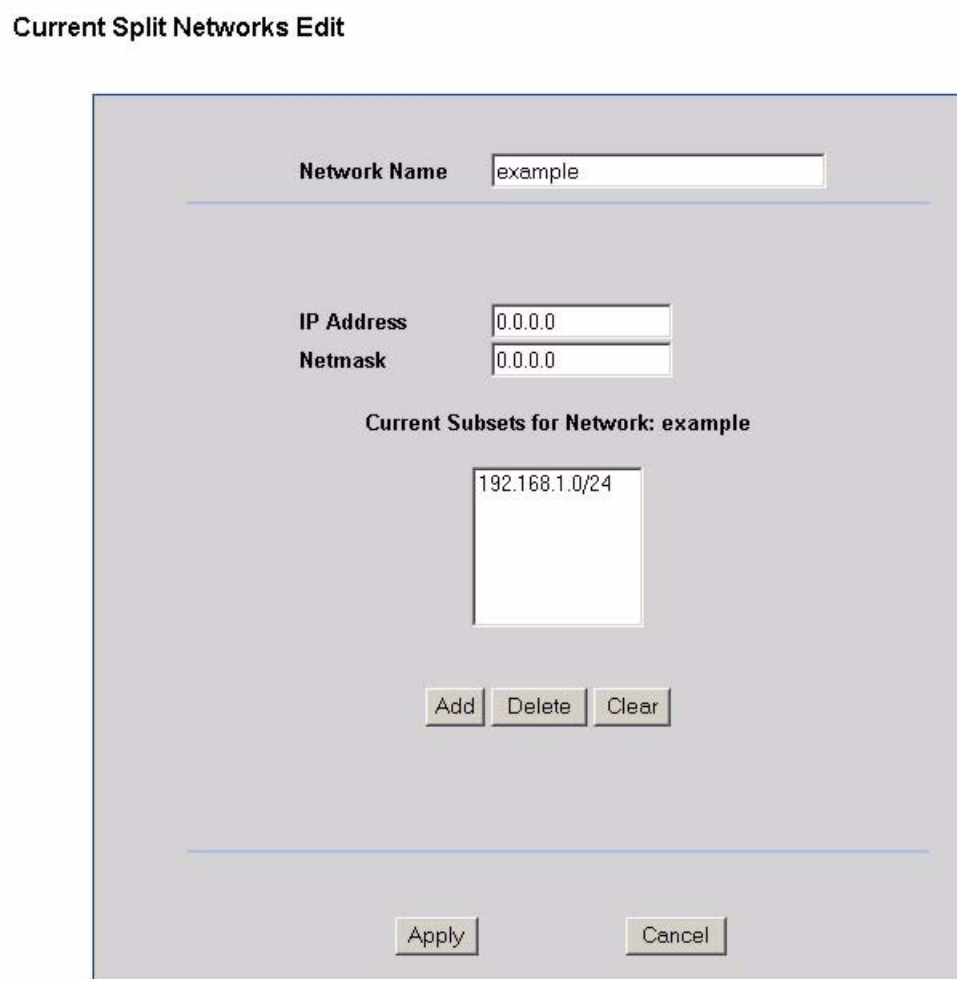


Table 89 describes the labels in Figure 109.

Table 89 Current split networks edit

Label	Description
Network Name	Enter a name to identify the split network.
IP Address	Enter the IP address for the split network in dotted decimal notation.
Netmask	Enter the netmask for the split network in dotted decimal notation.

Table 89 Current split networks edit

Label	Description
Current Subnets for Network:	This box displays the subnets that belong to this split network.
Add	Click **Add** to save your split network configuration.
Delete	Select a network subset and click **Delete** to remove it.
Clear	Click **Clear** to remove all of the configuration field and subnet settings.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Configuring RADIUS

Use RADIUS if you want to authenticate users using an external server.

To set up your Business Secure Router's RADIUS Server settings, click **AUTH SERVER,** then the **RADIUS** tab. The screen appears, as shown in Figure 110.

Figure 110 RADIUS

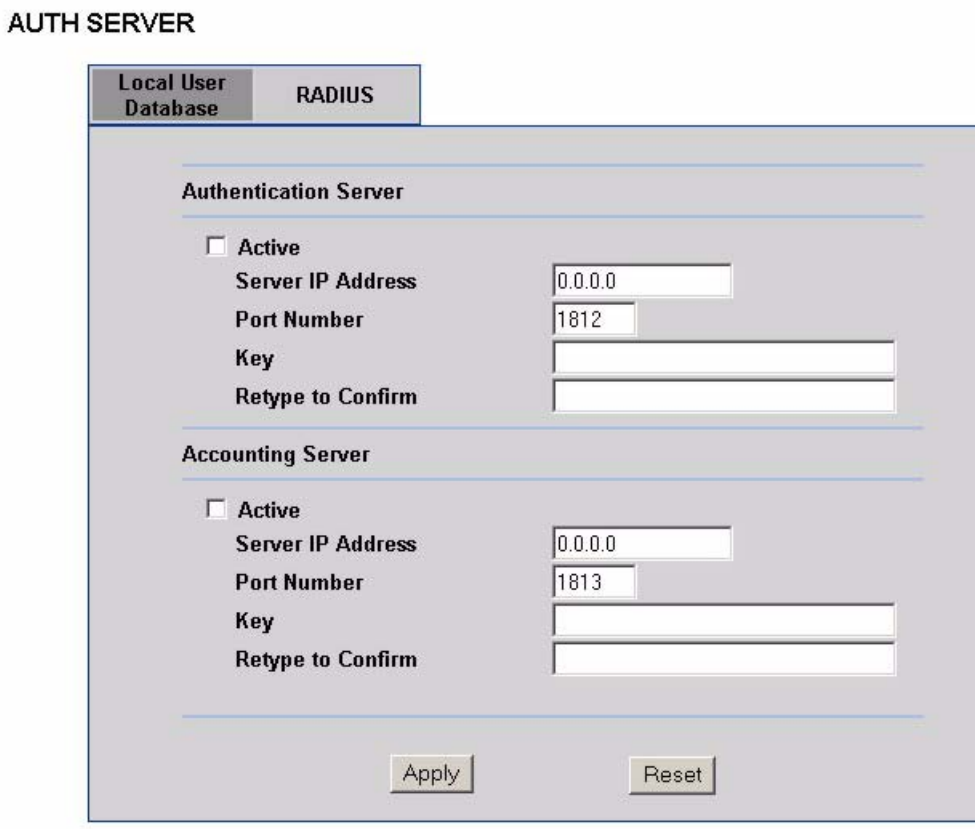


Table 90 describes the labels in Figure 110.

Table 90 RADIUS

Label	Description
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the Business Secure Router.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.

Table 90 RADIUS

Label	Description
Port Number	The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Business Secure Router. Note that, as you type a password, the screen displays an * for each character you type. The key is not sent over the network. This key must be the same on the external authentication server and Business Secure Router.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Business Secure Router. Note that as you type a password, the screen displays a (*) for each character you type. The key is not sent over the network. This key must be the same on the external accounting server and Business Secure Router.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 18
Remote management screens

This chapter provides information on the **Remote Management** screens.

Remote management overview

Remote management allows you to determine which services and protocols can access which Business Secure Router interface (if any) from which computers.

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You can manage your Business Secure Router from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable)

Note: If you choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Remote management limitations

Remote management over LAN or WAN does not work if:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.1.4 (WAN) is applied to block a Telnet, FTP, or Web service.
2. A service is disabled in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Business Secure Router disconnects the session immediately.
4. An SMT console session is running.
5. Another remote management session of the same type (web, FTP or Telnet) is running. You can only have one remote management session of the same type running at one time.
6. A web remote management session is running with a Telnet session. A web session is disconnected if you begin a Telnet session; nor does it begin if a Telnet session is already running.
7. A firewall rule blocks access to device.

Remote management and NAT

When NAT is enabled:

- Use the Business Secure Router's WAN IP address when configuring from the WAN.
- Use the Business Secure Router's LAN IP address when configuring from the LAN.

System timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or Telnet, web, or FTP connections. Your Business Secure Router automatically logs you off if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` was changed on the command line. Use the **System** screen to change the timeout period in the **Administrator Inactivity Timer** field.

Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts Web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party), and data integrity (you know if data has been changed).

HTTPS relies upon certificates, public keys, and private keys (see Chapter 14, "Certificates," on page 261 for more information).

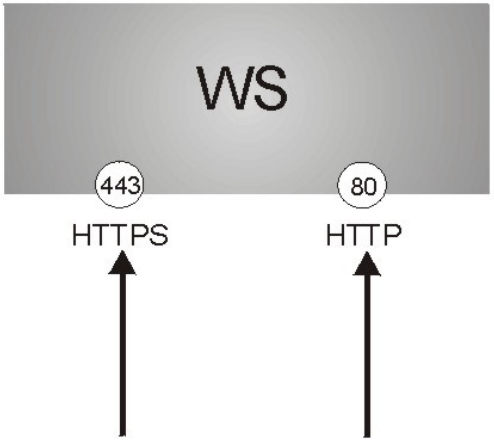
HTTPS on the Business Secure Router is used so that you can securely access the Business Secure Router using the WebGUI. The SSL protocol specifies that the SSL server (the Business Secure Router) must always authenticate itself to the SSL client (the computer that requests the HTTPS connection with the Business Secure Router), whereas the SSL client only authenticates itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT**, **WWW** screen). **Authenticate Client Certificates** is optional and, if selected, means the SSL-client must send the Business Secure Router a certificate. You must apply for a certificate for the browser from a trusted CA on the Business Secure Router.

Refer to Figure 111 about HTTPS implementation.

1 HTTPS connection requests from an SSL-aware Web browser go to port 443 (by default) on the Business Secure Router's WS (Web server).

2 HTTP connection requests from a Web browser go to port 80 (by default) on the Business Secure Router's WS (Web server).

Figure 111 HTTPS implementation



Note: If you disable **HTTP Server Access** (**Disable**) in the **REMOTE MGMT WWW** screen, the Business Secure Router blocks all HTTP connection attempts.

Configuring WWW

To change your Business Secure Router's Web settings, click **REMOTE MGMT** to open the **WWW** screen.

Figure 112 WWW

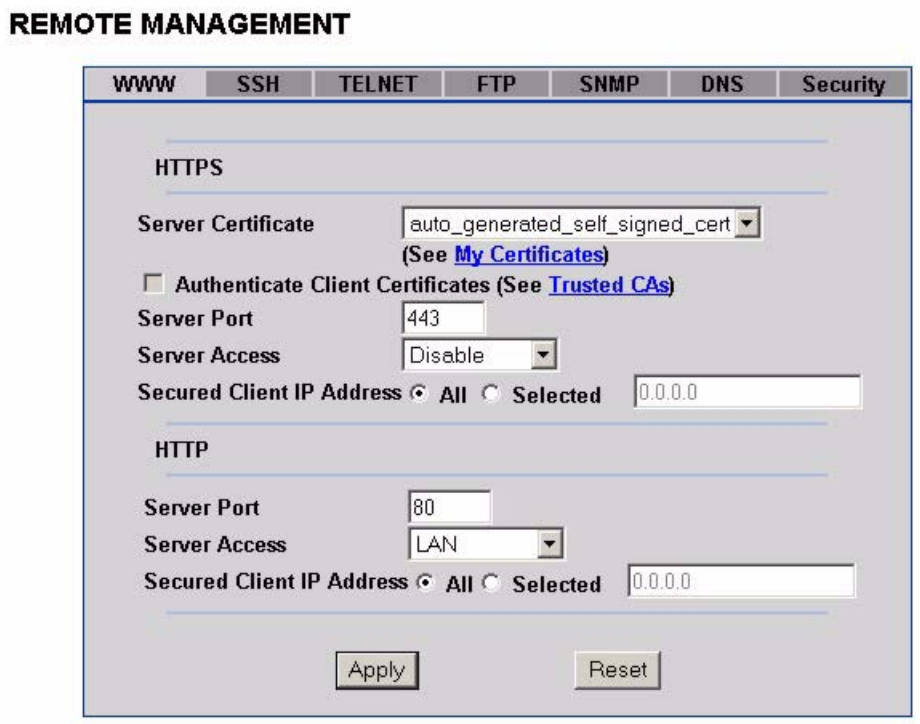


Table 91 describes the labels in Figure 112.

Table 91 WWW

Label	Description
HTTPS	
Server Certificate	Select the **Server Certificate** that the Business Secure Router uses to identify itself. The Business Secure Router is the SSL server and must always authenticate itself to the SSL client (the computer that requests the HTTPS connection with the Business Secure Router).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the Business Secure Router by sending the Business Secure Router a certificate. To do that, the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Business Secure Router (see the appendix on importing certificates for details).

Table 91 WWW

Label	Description
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the Business Secure Router, for example, 8443, you must notify people who need to access the Business Secure Router WebGUI to use https://Business Secure Router IP Address:8443 as the URL.
Server Access	Select a Business Secure Router interface from **Server Access** on which incoming HTTPS access is allowed. You can allow only secure WebGUI access by setting the **HTTP Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
HTTP	
Server Port	You can change the server port number for a service, if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the Business Secure Router using this service.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

HTTPS example

To change the default HTTPS port on the Business Secure Router, in your browser, enter “https://Business Secure Router IP Address/” as the Web site address, where “Business Secure Router IP Address” is the IP address or domain name of the Business Secure Router you wish to access.

Internet Explorer warning messages

When you attempt to access the Business Secure Router HTTPS server, a Windows dialog box appears, asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Business Secure Router.

The **Security Alert** screen shown in Figure 113 appears in Internet Explorer. Select **Yes** to proceed to the WebGUI logon screen; if you select **No**, then WebGUI access is blocked.

Figure 113 Security Alert dialog box (Internet Explorer)

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No
View Certificate

Netscape Navigator warning messages

When you attempt to access the Business Secure Router HTTPS server, a **Website Certified by an Unknown Authority** screen (shown in Figure 114) appears asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Business Secure Router.

If you select **Accept this certificate temporarily for this session**, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Business Secure Router's certificate into the SSL client.

Figure 114 Figure 18-4 Security Certificate 1 (Netscape)

Website Certified by an Unknown Authority
Unable to verify the identity of
Factory Default Certificate as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be
actory Default Certificate,
possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site
Factory Default Certificate?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 115 Security Certificate 2 (Netscape)

Security Error: Domain Name Mismatch
You have attempted to establish a connection with "192.168.1.1". However, the security certificate presented belongs to '
Factory Default Certificate". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "192.168.1.1", please cancel the connection and notify the site administrator.
View Certificate
OK
Cancel
Help

Avoiding the browser warning messages

The following section describes the main reasons that your browser displays warnings about the Business Secure Router's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the Business Secure Router's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Business Secure Router's factory default certificate is the Business Secure Router itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.
- The actual IP address of the HTTPS server (the IP address of the Business Secure Router's port that you are trying to access) does not match the common name specified in the Business Secure Router's HTTPS server certificate that your browser received. To check the common name specified in the certificate that your Business Secure Router sends to HTTPS clients:

a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

b Click **CERTIFICATES**. Find the certificate that was displayed in the Server Certificate field and check its **Subject** column. **CN** stands for certificate's common name (see Figure 119 on page 340 for an example).

Use this procedure to have the Business Secure Router use a certificate with a common name that matches the Business Secure Router's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

a Create a new certificate for the Business Secure Router that uses the IP address (of the Business Secure Router's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.

b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

Logon screen

After you accept the certificate, the Business Secure Router logon screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 116 Logon screen (Internet Explorer)

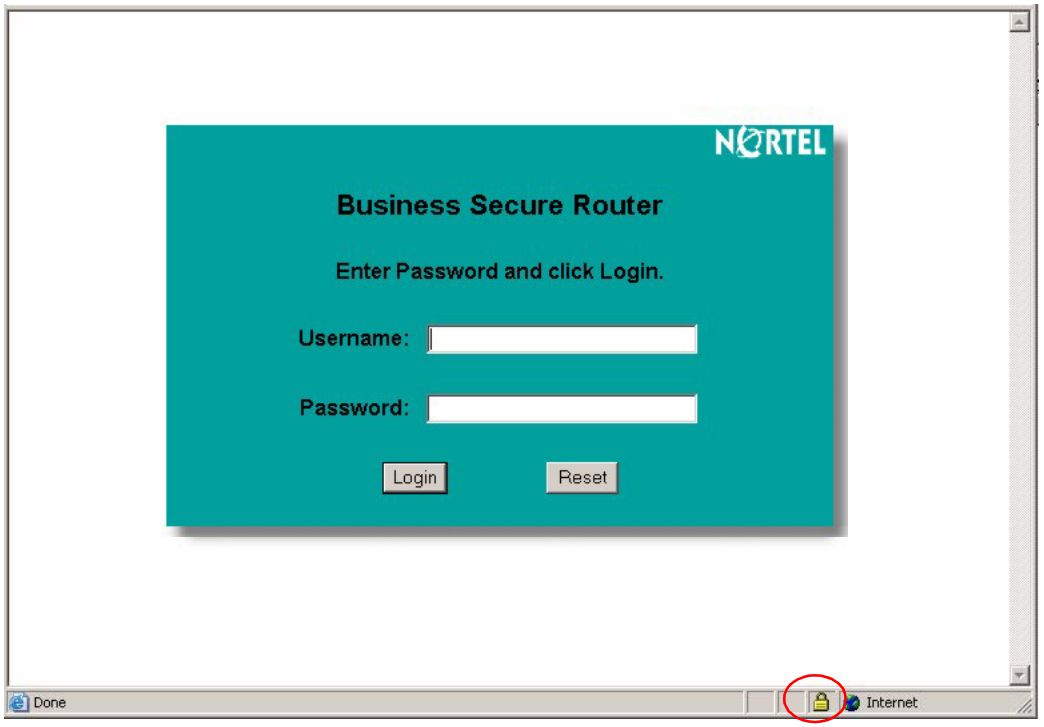
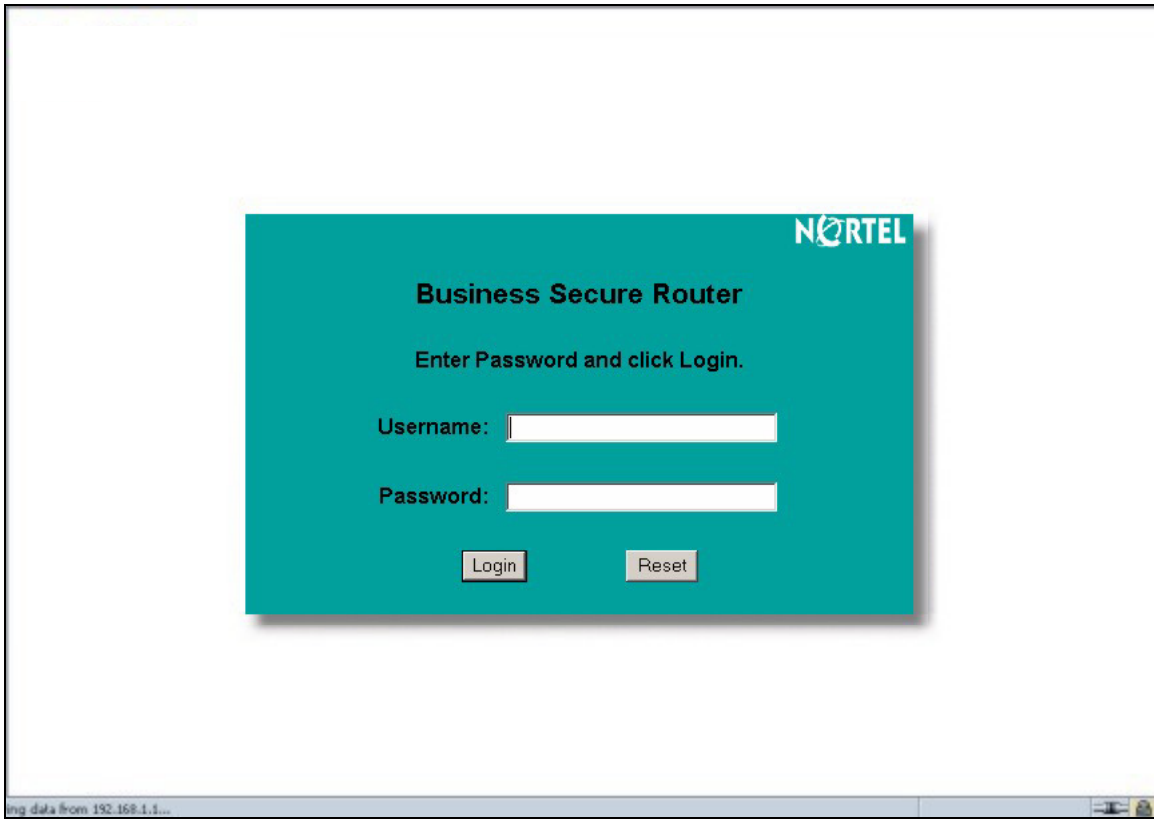


Figure 117 Login screen (Netscape)



Click **Login** to proceed. The screen shown in Figure 118 appears.

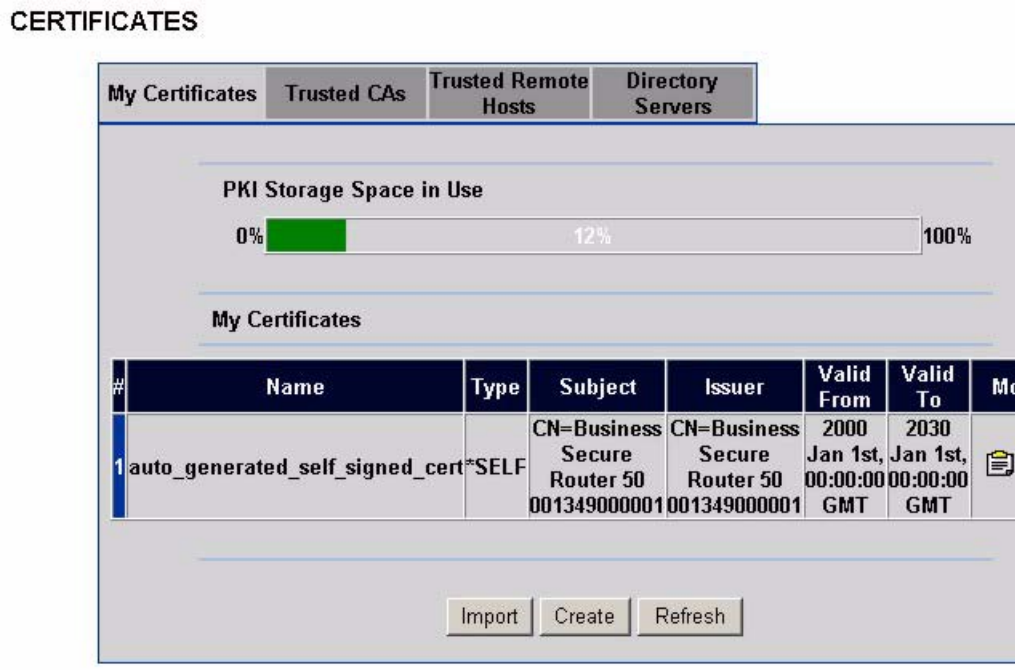
The factory default certificate is a common default certificate for all Business Secure Router models.

Figure 118 Replace certificate

NORTEL
Replace Factory Default Certificate
The factory default certificate is common to Business Secure Router series models. Click Apply to create a certificate using your Business Secure Router 's MAC address that will be specific to this device.
Apply
Ignore

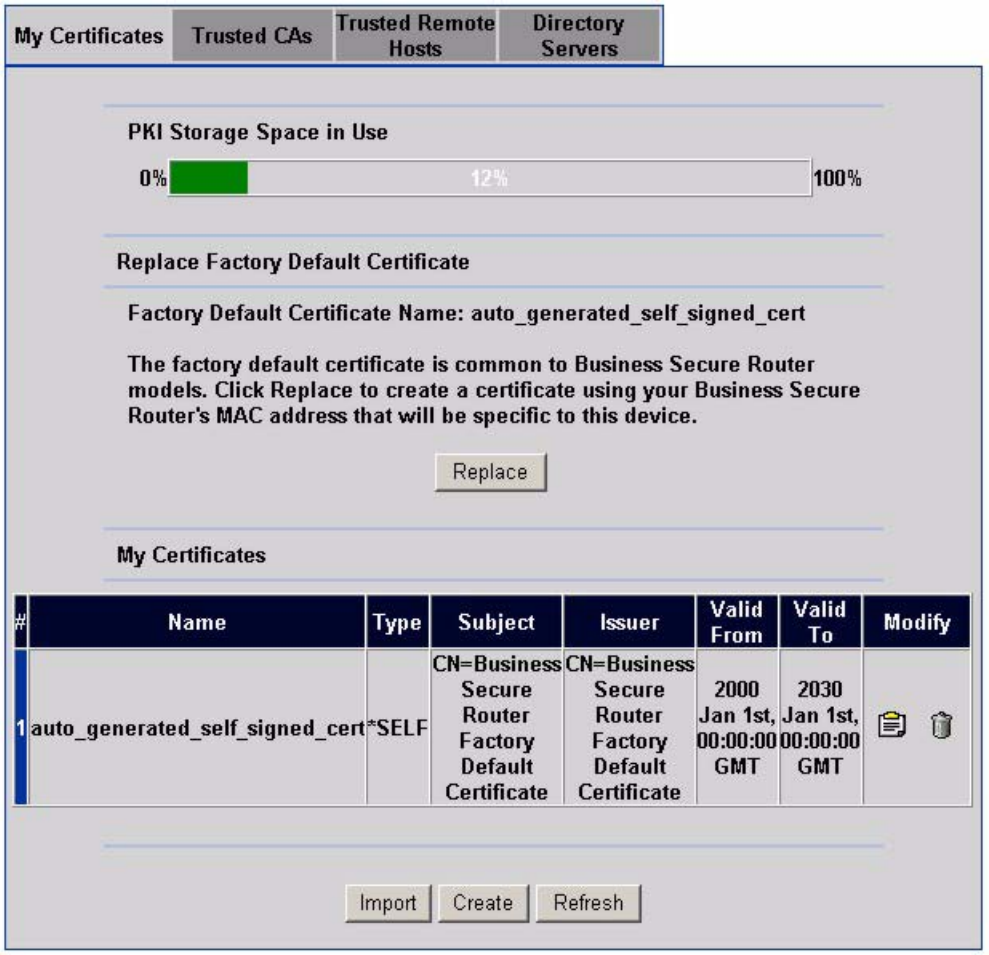
Click **Apply** in the **Replace Certificate** screen to create a certificate using your Business Secure Router's MAC address that is specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You see information similar to that shown in Figure 119.

Figure 119 Device-specific certificate



Click **Ignore** in the **Replace Certificate** screen to use the common Business Secure Router certificate. The **My Certificates** screen appears (Figure 120).

Figure 120 Common Business Secure Router certificate


My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
12%
100%
Replace Factory Default Certificate
Factory Default Certificate Name: auto_generated_self_signed_cert
The factory default certificate is common to Business Secure Router models. Click Replace to create a certificate using your Business Secure Router's MAC address that will be specific to this device.
Replace
My Certificates
Name Type Subject Issuer Valid From Valid To Modify
1 auto_generated_self_signed_cert *SELF CN=Business Secure Router Factory Default Certificate CN=Business Secure Router Factory Default Certificate 2000 Jan 1st, 00:00:00 GMT 2030 Jan 1st, 00:00:00 GMT
Import
Create
Refresh

SSH overview

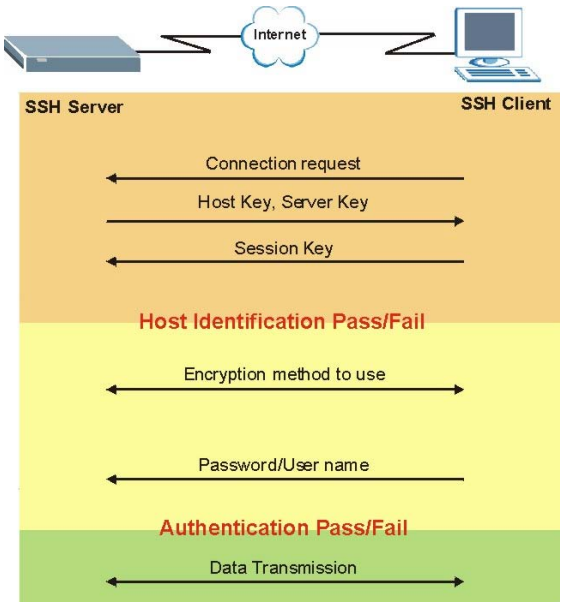
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 121 SSH Communication Example

How SSH works

Figure 122 summarizes how a secure connection is established between two remote hosts.

Figure 122 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (username and password) to the server to log on to the server.

SSH implementation on the Business Secure Router

Your Business Secure Router supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Business Secure Router for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

Requirements for using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Business Secure Router over SSH.

Configuring SSH

To change your Business Secure Router's Secure Shell settings, click **REMOTE MGMT**, and then the **SSH** tab. The screen shown in Figure 123 appears.

Figure 123 SSH

Table 92 describes the labels in Figure 123.

Table 92 SSH

Label	Description
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the Business Secure Router for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 14, “Certificates,” on page 261for details).
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the Business Secure Router using this service.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Note: Nortel recommends that you disable Telnet and FTP when you configure SSH for secure connections.

Secure Telnet using SSH examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Business Secure Router. The configuration and connection steps are similar for most SSH client programs. For more information about SSH client programs, refer to your SSH client program user's guide.

Example 1: Microsoft Windows

This section describes how to access the Business Secure Router using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number, or device name) for the Business Secure Router.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window appears, prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 124 SSH Example 1: Store Host Key

Host Identification
You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.
The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"
You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.
Do you want to save the new host key to the local database?
Yes
No
Cancel
Help

Enter the password to log on to the Business Secure Router. The SMT main menu appears.

Example 2: Linux

This section describes how to access the Business Secure Router using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the Business Secure Router.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the Business Secure Router (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the Business Secure Router.

Figure 125 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the Business Secure Router using SSH version 1. If this is the first time you are connecting to the Business Secure Router using SSH, a message appears prompting you to save the host information of the Business Secure Router. Type yes and press [ENTER].

Enter the password to log on to the Business Secure Router.

Figure 126 SSH Example 2: Log on

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
```

3 The SMT main menu displays.

Secure FTP using SSH example

This section shows an example of file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. For more information about using FTP, refer to your SSH client program user's guide.

1 Enter `sftp -1 192.168.1.1`. This command forces your computer to connect to the Business Secure Router for secure file transfer using SSH version 1. If this is the first time you are connecting to the Business Secure Router using SSH, a message displays, prompting you to save the host information of the Business Secure Router. Type `yes` and press [ENTER].

2 Enter the password to log on to the Business Secure Router.

3 Use the `put` command to upload a new firmware to the Business Secure Router.

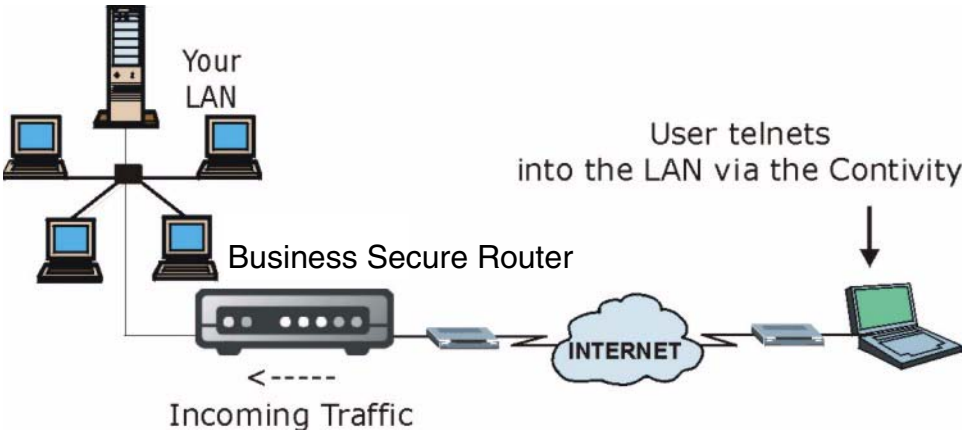
Figure 127 Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

Telnet

You can configure your Business Secure Router for remote Telnet access as shown in Figure 128.

Figure 128 Telnet configuration on a TCP/IP network



Configuring TELNET

Click **REMOTE MANAGEMENT** to open the **TELNET** screen.

Figure 129 Telnet

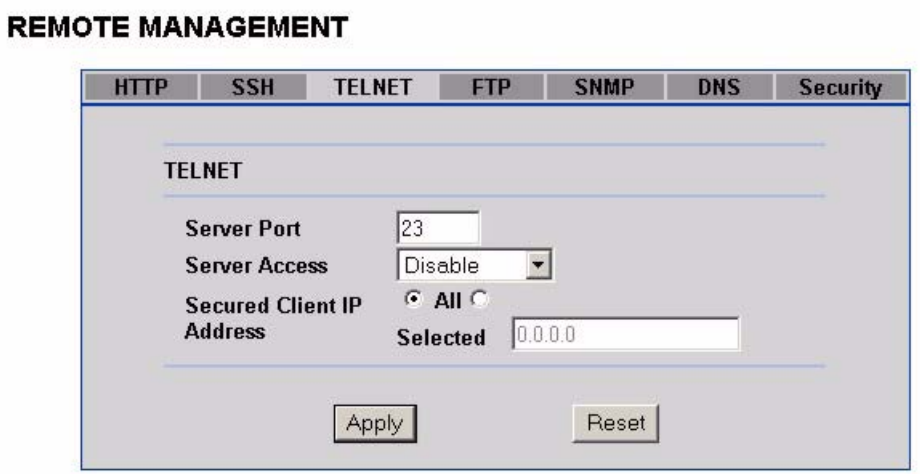


Table 93 describes the fields in Figure 129.

Table 93 Telnet

Label	Description
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the Business Secure Router using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring FTP

You can upload and download the Business Secure Router's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

To change your Business Secure Router's FTP settings, click **REMOTE MANAGEMENT**, and then the **FTP** tab. The screen appears as shown in Figure 130.

Figure 130 FTP

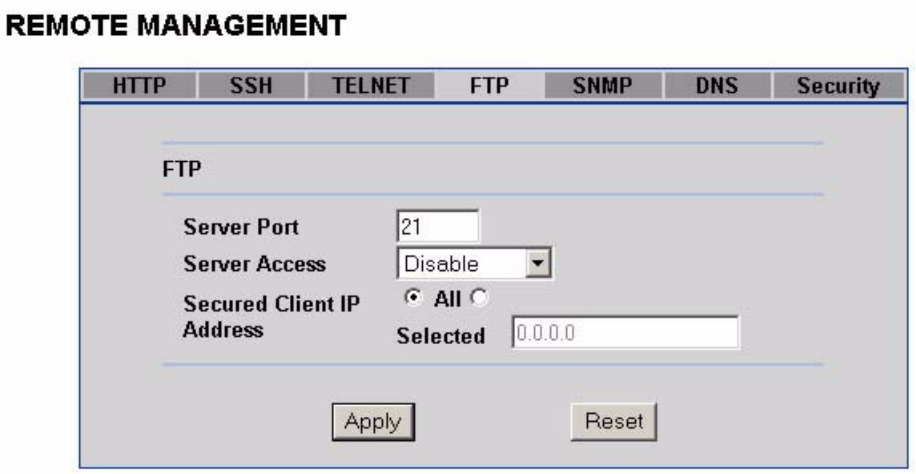


Table 94 describes the fields in Figure 130.

Table 94 FTP

Label	Description
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the Business Secure Router using this service.

Table 94 FTP

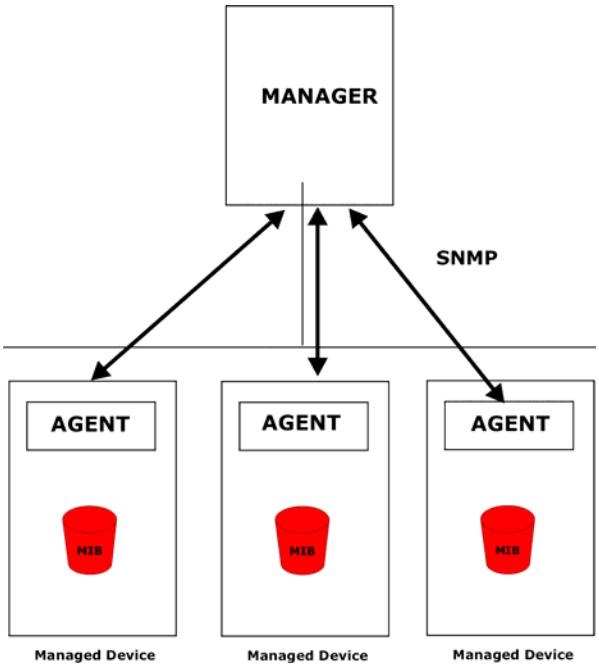
Label	Description
Secured Client IP Address	A secured client is a trusted computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Business Secure Router supports SNMP-agent functionality, which allows a manager station to manage and monitor the Business Secure Router through the network. The Business Secure Router supports SNMP version 1 (SNMPv1). Figure 131 illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured. The default get and set communities are public.

Note: SNMP is only available if TCP/IP is configured.

Figure 131 SNMP Management Model



An SNMP-managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Business Secure Router). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables and managed objects that define each piece of information to be collected about a device. Examples of variables include number of packets received and node port status. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request and response protocol based on the manager and agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get-Allows the manager to retrieve an object variable from the agent.
- GetNext-Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set-Allows the manager to set values for object variables within an agent.
- Trap -Used by the agent to inform the manager of some events.

Supported MIBs

The Business Secure Router supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

SNMP Traps

The Business Secure Router sends traps to the SNMP manager when any one of the following events occurs:

Table 95 SNMP traps

Trap #	Trap Name	Description
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message System reboot by user! if reboot is done intentionally, (for example, download new files, and CI command sys reboot).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

REMOTE MANAGEMENT: SNMP

To change your Business Secure Router's SNMP settings, click **REMOTE MANAGEMENT**, and then the **SNMP** tab. The screen appears as shown in Figure 132.

Figure 132 SNMP

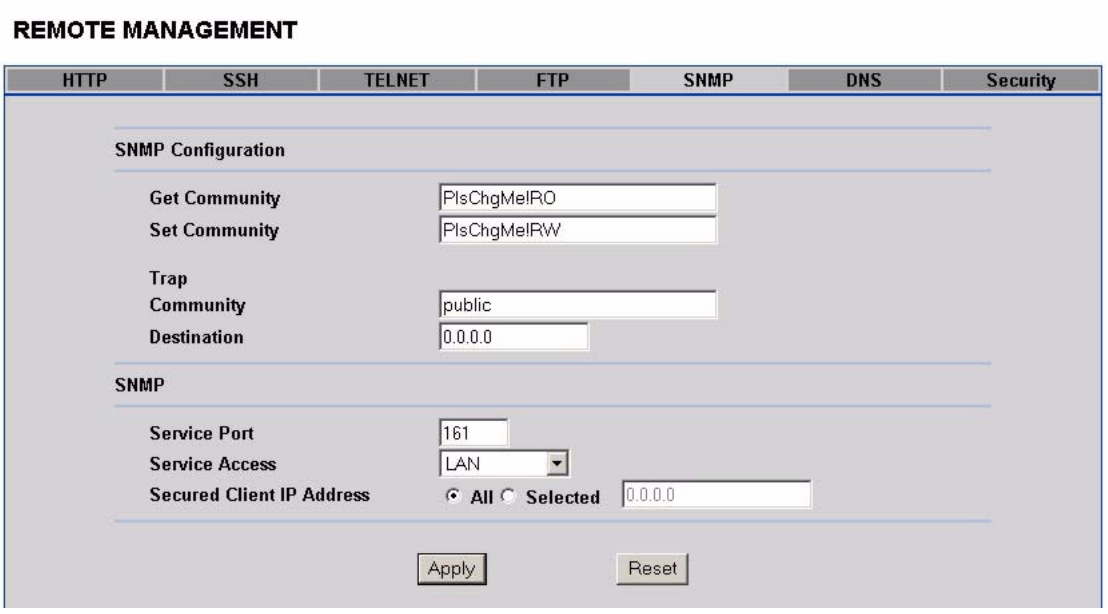


Table 96 describes the fields in Figure 132.

Table 96 SNMP

Label	Description
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is "PlsChgMe!RO".
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is "PlsChgMe!RW".

Table 96 SNMP

Label	Description
Trusted Host	If you enter a trusted host, your Business Secure Router only responds to SNMP messages from this address. In the field, 0.0.0.0 (default) means your Business Secure Router responds to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Service Access	Select the interfaces (If any) through which a computer can access the Business Secure Router using this service.
Secured Client IP Address	A secured client is a trusted computer that is allowed to communicate with the Business Secure Router using this service. Select **All** to allow any computer to access the Business Secure Router using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Business Secure Router using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.nortel.com is 47.249.48.20.

To change your Business Secure Router's DNS settings, click **REMOTE MANAGEMENT**, and then the **DNS** tab. The screen appears as shown in Figure 133.

Figure 133 DNS

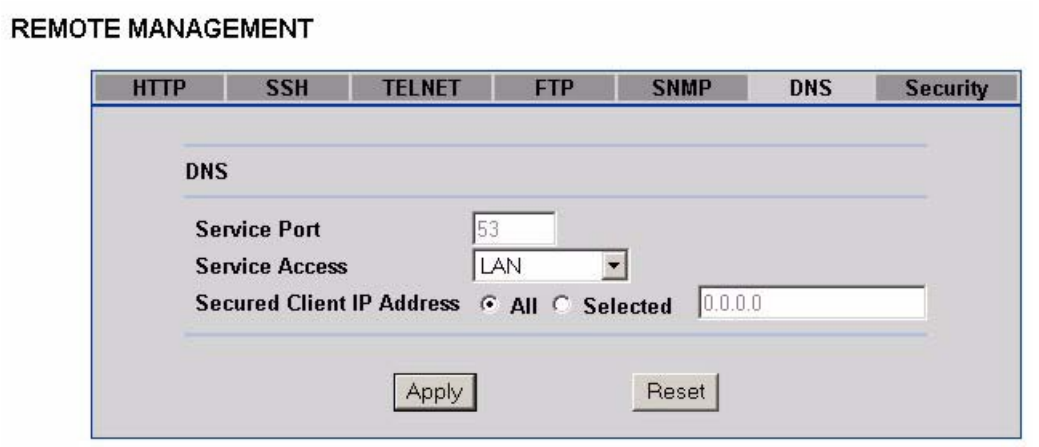


Table 97 describes the fields in Figure 133.

Table 97 DNS

Label	Description
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interfaces (if any) through which a computer can send DNS queries to the Business Secure Router.
Secured Client IP Address	A secured client is a trusted computer that is allowed to send DNS queries to the Business Secure Router. Select **All** to allow any computer to send DNS queries to the Business Secure Router. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the Business Secure Router.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Security

To change your Business Secure Router's Security settings, click **REMOTE MANAGEMENT**, and then the **Security** tab. The screen appears as shown in Figure 134.

If an outside user attempts to probe an unsupported port on your Business Secure Router, an ICMP response packet is automatically returned. This allows the outside user to know the Business Secure Router exists. The Business Secure Router series support antiprobing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Business Secure Router when unsupported ports are probed.

Note: In order to allow Ping on the WAN, you must also configure a WAN to WAN/ Business Secure Router rule that allows PING(ICMP:0) traffic.

Figure 134 Security

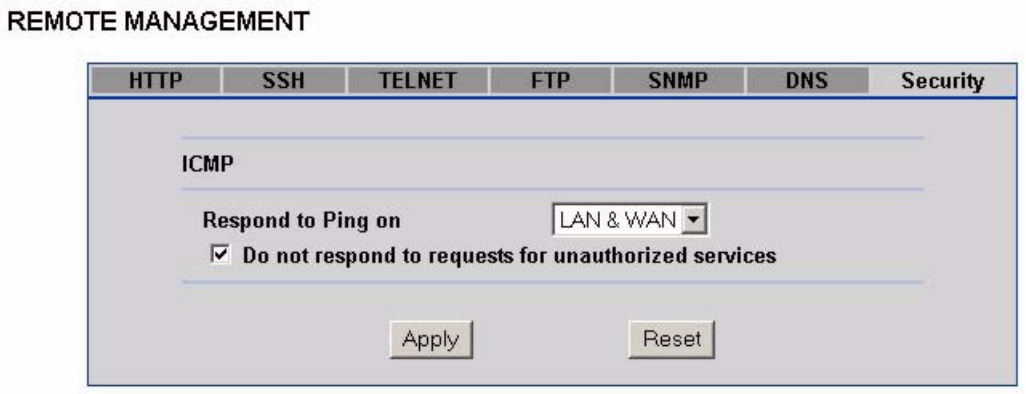


Table 98 describes the fields in Figure 134.

Table 98 Security

Label	Description
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The Business Secure Router does not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise, select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.

Table 98 Security

Label	Description
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the Business Secure Router by probing for unused ports. If you select this option, the Business Secure Router does not send ICMP response packets to port requests for unused ports, thus leaving the unused ports and the Business Secure Router unseen. If the firewall blocks a packet from the WAN, the Business Secure Router sends a TCP reset packet. Use the sys firewall tcprst rst off command in the command interpreter if you want to stop the Business Secure Router from sending TCP reset packets.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 19
UPnP

This chapter introduces the Universal Plug and Play feature.

Universal Plug and Play overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

How do I know if I am using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network appears as a separate icon. By selecting the icon of a UPnP device, you can access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices, and enable exchange of simple product and service descriptions. With NAT traversal, the device can do the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports can present network security issues. Network information and configuration can also be obtained and modified by users in some network environments.

All UPnP-enabled devices can communicate freely with each other without additional configuration. If this is not your intention, disable UPnP.

UPnP implementation

The device has UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). This UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing, the UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

The Business Secure Router only sends UPnP multicasts to the LAN.

Configuring UPnP

Click **UPnP** to display the screen shown in Figure 135.

Figure 135 Configuring UPnP

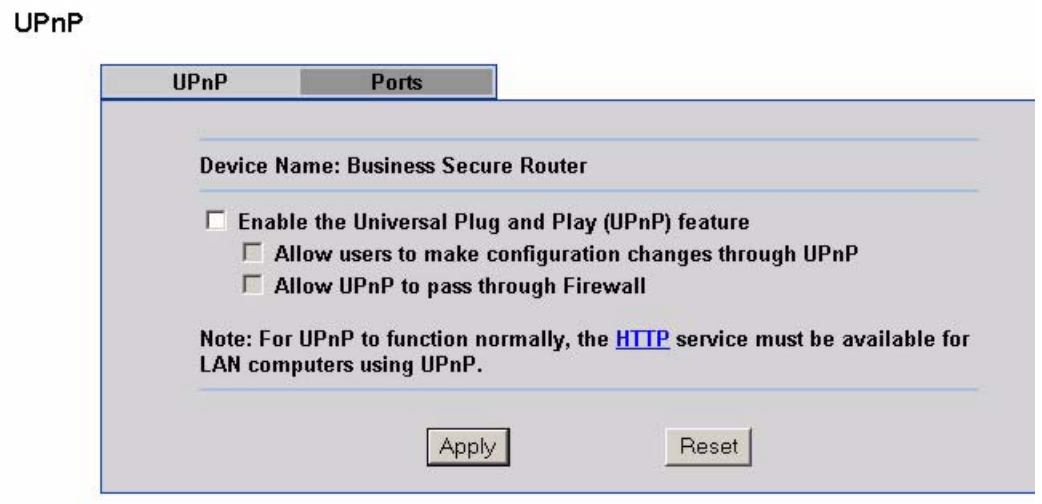

UPnP
UPnP
Ports
Device Name: Business Secure Router
Enable the Universal Plug and Play (UPnP) feature
Allow users to make configuration changes through UPnP
Allow UPnP to pass through Firewall
Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Apply
Reset

Table 99 describes the fields in Figure 135.

Table 99 Configuring UPnP

Label	Description
Device Name	This identifies the device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone can use a UPnP application to open the WebGUI's logon screen without entering the Business Secure Router's IP address (although you must still enter the password to access the WebGUI).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Business Secure Router so that they can communicate through the Business Secure Router. For example, by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; eliminating the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Displaying UPnP port mapping

Click **UPnP** and then **Ports** to display the screen as shown in Figure 136. Use this screen to view the NAT port mapping rules that UPnP creates on the Business Secure Router.

Figure 136 UPnP Ports

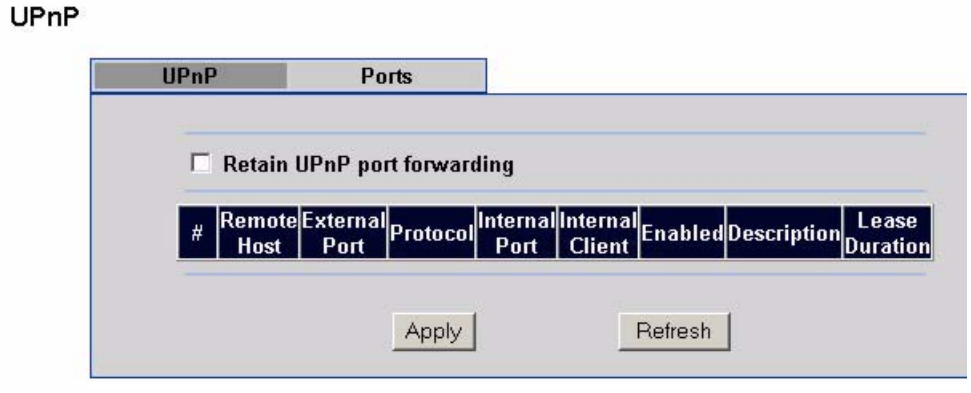


Table 100 describes the labels in Figure 136.

Table 100 UPnP Ports

Label	Description
Retain UPnP port forwarding	Select this check box to have the Business Secure Router retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example, FTP for file transfers), the Business Secure Router can keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the Business Secure Router's NAT routing table.	
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Because this is often a wildcard, the field can be blank. When the field is blank, the Business Secure Router forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the Business Secure Router forward inbound packets to the **Internal Client** from that IP address only.

Table 100 UPnP Ports

Label	Description
External Port	This field displays the port number that the Business Secure Router listens on (on the WAN port) for connection requests destined for the NAT rule's **Internal Port** and **Internal Client**. The Business Secure Router forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays "0", the Business Secure Router ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the **Internal Client** to which the Business Secure Router forwards incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the Business Secure Router and configured the UPnP-created NAT mapping rule on the Business Secure Router determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays a dynamic port-mapping rule's time to live (in seconds). It displays "0" if the port mapping is static.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Refresh	Click **Refresh** to update the screen's table.

Installing UPnP in Windows example

This section shows how to install UPnP in Windows Me and Windows XP.

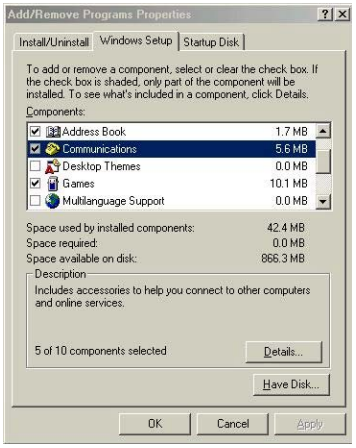
Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 137 Add/Remove programs: Windows setup

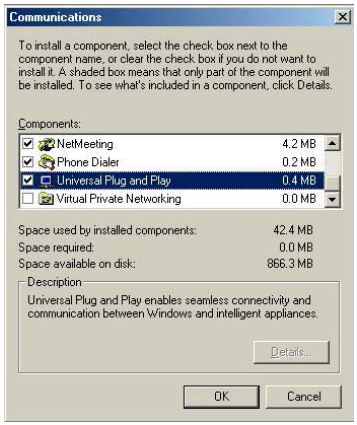

Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

4 Click **OK** to return to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Figure 138 Communications


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

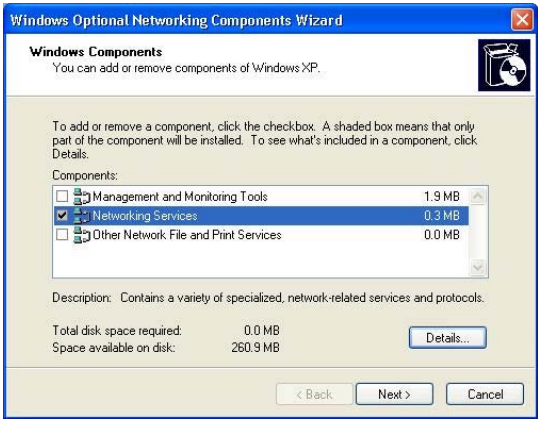
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window appears.

Figure 139 Network connections

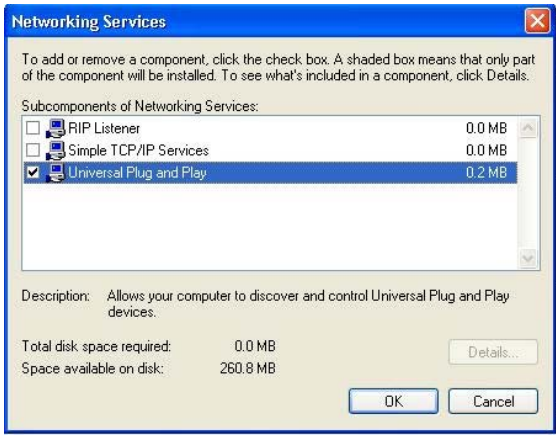
4 Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 140 Windows optional networking components wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 141 Windows XP networking services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to return to the **Windows Optional Networking Component Wizard** window and click **Next**.

Using UPnP in Windows XP example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the device.

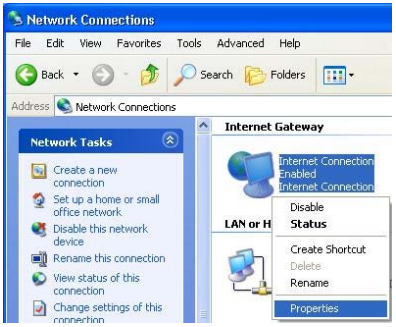
Make sure the computer is connected to a LAN port of the device. Turn on your computer and the Business Secure Router.

Autodiscover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 142 Internet gateway icon



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

Figure 143 Internet connection properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You can edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 144 Internet connection properties advanced setup

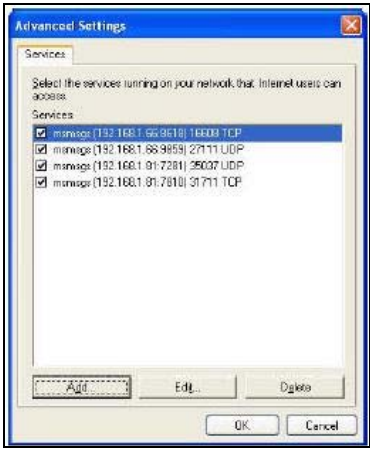
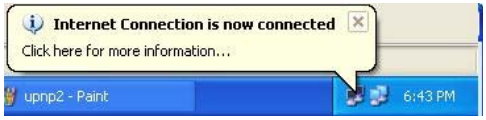


Figure 145 Service settings

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings are deleted automatically.

5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.

Figure 146 Internet connection icon



6 Double-click the icon to display your current Internet connection status.

Figure 147 Internet connection status

WebGUI easy access

With UPnP, you can access the WebGUI without first finding out its IP address. This is helpful if you do not know the IP address of your Business Secure Router.

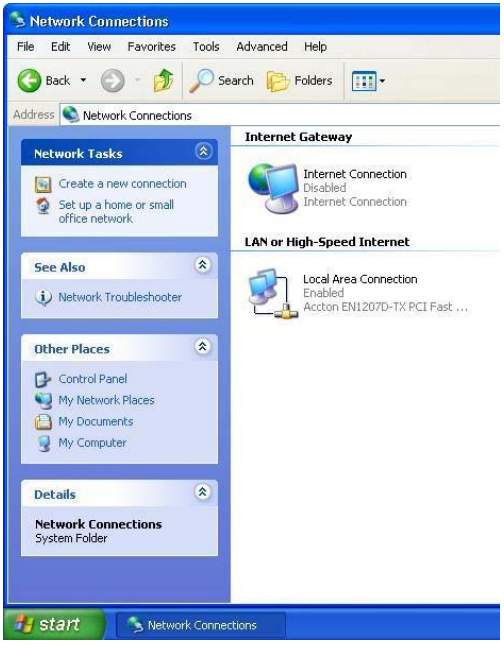
Follow the steps below to access the WebGUI.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**

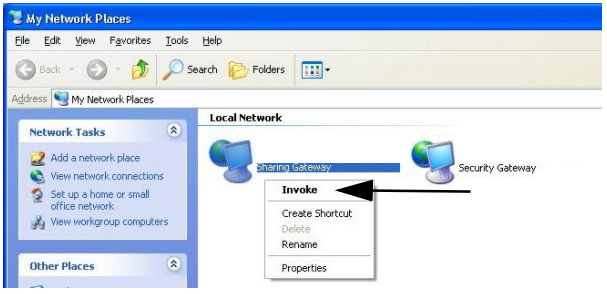
Figure 148 Network connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click the icon for your Business Secure Router and select **Invoke**. The WebGUI logon screen displays.

Figure 149 My Network Places: Local network



Chapter 20
Logs Screens

This chapter contains information about configuring general log settings and viewing the Business Secure Router's logs. Refer to Appendix B, "Log Descriptions," on page 423 for example log message explanations.

Configuring View Log

With the WebGUI, you can look at all of the Business Secure Router's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see "Configuring Log settings" on page 373). Options include logs about system maintenance, system errors, access control, allowed or blocked Web sites, blocked Web features (such as ActiveX controls, Java and cookies), attacks (such as DoS), and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 150 View Log

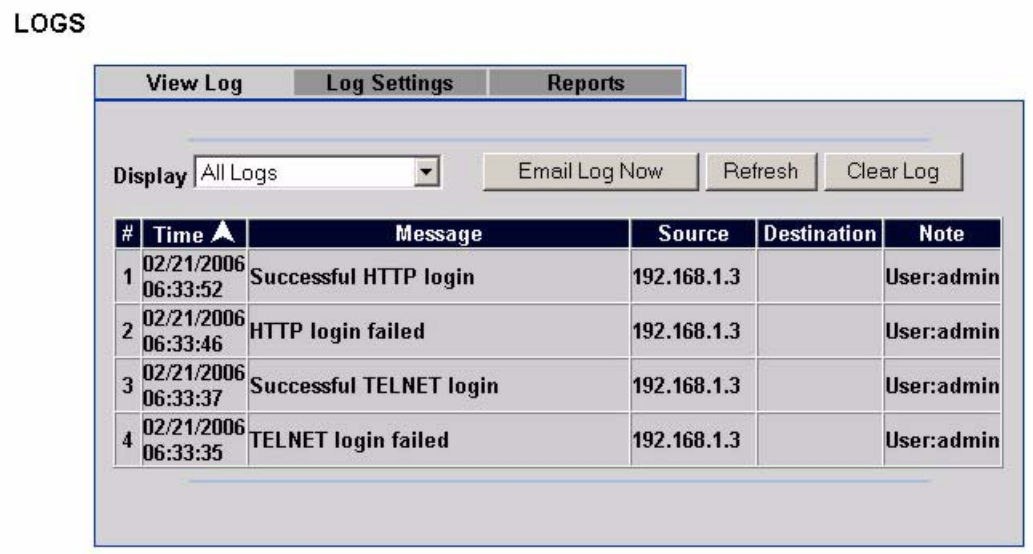


Table 101 describes the fields in Figure 150.

Table 101 View Log

Label	Description
Display	The categories that you select in the **Log Settings** page display in the drop-down list. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. Refer to "Configuring Time and Date" on page 86 for information about configuring the Business Secure Router's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).

Table 101 View Log

Label	Description
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

Configuring Log settings

To change your Business Secure Router's log settings, click **Logs**, then the **Log Settings** tab. The screen appears as shown in Figure 151.

Use the **Log Settings** screen to configure to where the Business Secure Router sends logs; the schedule for when the Business Secure Router is to send the logs and which logs and immediate alerts the Business Secure Router is to send.

An alert is a type of log that warrants more serious attention including system errors, attacks (access control), and attempted access to blocked Web sites or Web sites with restricted Web features such as cookies, Active X, and so on. Some categories, such as **System Errors,** consist of both logs and alerts. You can differentiate between logs and alerts by their color in the **View Log** screen. Alerts display in red and logs display in black.

Note: Alerts are e-mailed as soon as they happen. Logs can be e-mailed as soon as the log is full. Selecting many alert and log categories (especially Access Control) can result in many e-mails being sent.

Figure 151 Log settings

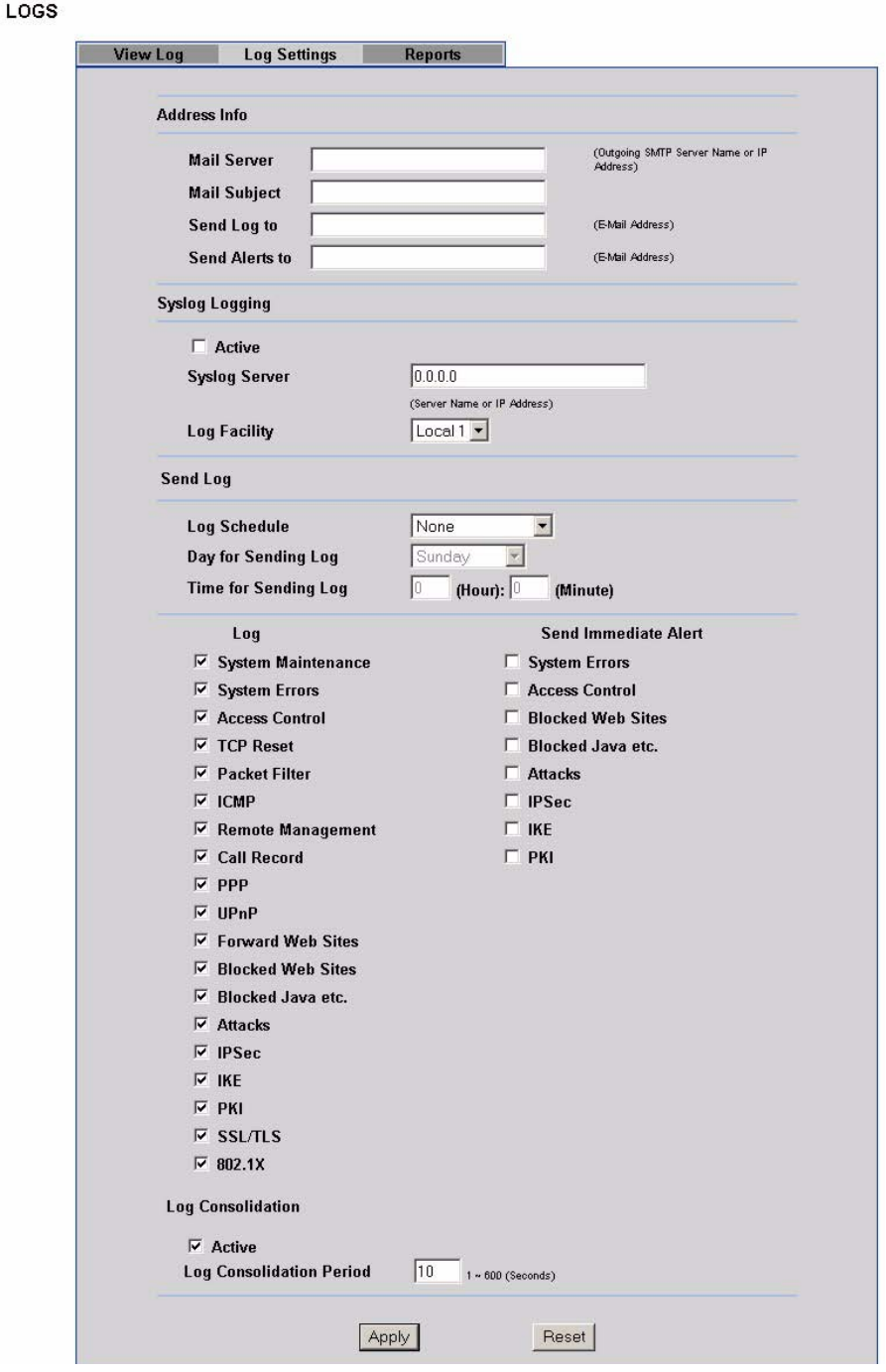


Table 102 describes the fields in Figure 151.

Table 102 Log settings

Label	Description
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages are not sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the Business Secure Router sends.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs are not sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts are not sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that logs the selected categories of logs.
Log Facility	Select a location from the drop-down list. In the log facility, you can log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as e-mail: Daily Weekly Hourly When the Log is Full None If you select **Weekly** or **Daily**, specify a time of day when the e-mail will be sent. If you select **Weekly**, you must also specify which day of the week the e-mail is to be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop-down list to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 p.m.) to send the logs.

Table 102 Log settings

Label	Description
Log	Select the categories of the logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the Business Secure Router to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) can be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. You can use the `sys log consolidate msglist` command to see which log messages are consolidated.
Log Consolidation Period	Specify the time interval during which to merge logs with identical messages into one log.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Reports

To change your Business Secure Router's log reports, click **Logs**, and then the **Reports** tab. The screen appears as shown in Figure 152.

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most, and which Web sites are visited the most often. Use the **Reports** screen to have the Business Secure Router record and display the following network usage details:

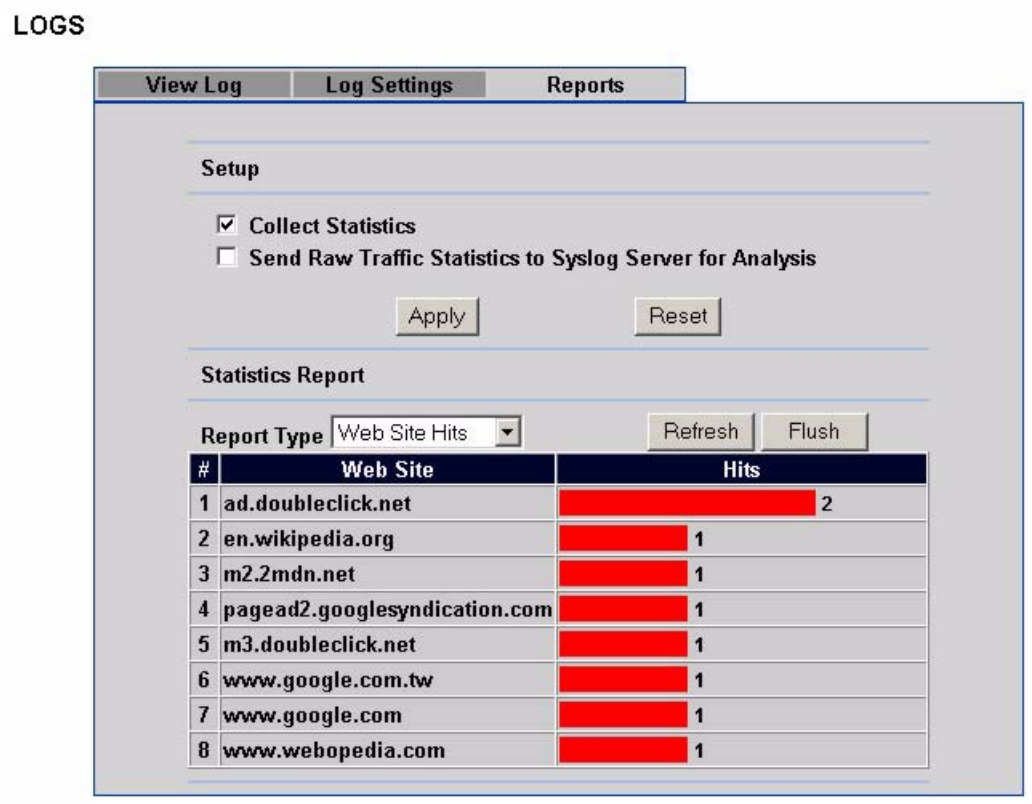
- Web sites visited the most often
- Number of times the most visited Web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and from which the most traffic has been sent

- How much traffic has been sent to and from the LAN IP addresses to and from which the most traffic has been sent

Note: The Web site hit count not be 100% accurate because sometimes when an individual Web page loads, it can contain references to other Web sites that also get counted as hits.

The Business Secure Router records Web site hits by counting the HTTP GET packets. Many Web sites include HTTP GET references to other Web sites and the Business Secure Router can count these as hits, thus the Web hit count is not (yet) 100% accurate.

Figure 152 Reports



Note: Enabling the Business Secure Router's reporting function decreases the overall throughput by about 1 Mb/s.

Table 103 describes the fields in Figure 152.

Table 103 Reports

Label	Description
Collect Statistics	Select the check box and click **Apply** to have the Business Secure Router record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click **Apply** to have the Business Secure Router send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the **Log Settings** screen.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Reset	Click **Reset** to begin configuring this screen afresh.
Report Type	Use the drop-down list to select the type of reports to display. **Web Site Hits** displays the Web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **LAN IP Address** displays the LAN IP addresses to and from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
Flush	Click **Flush** to discard the old report data and update the report display.

Note: All of the recorded reports data is erased when you turn off the Business Secure Router.

Viewing Web site hits

In the Reports screen, select **Web Site Hits** from the **Report Type** drop-down list to have the Business Secure Router record and display which Web sites have been visited the most often and how many times they have been visited.

Figure 153 Web site hits report example

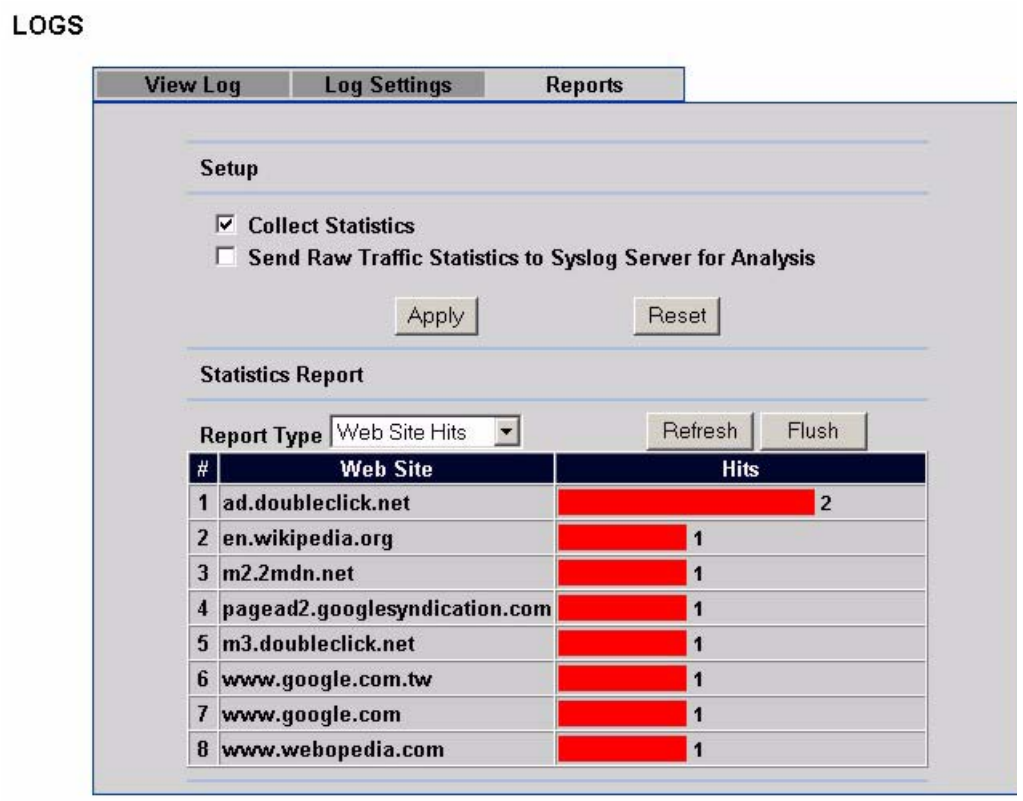


Table 104 describes the fields in Figure 153.

Table 104 Web site hits report

Label	Description
Web Site	This column lists the domain names of the Web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each Web site and listed in descending order with the most visited Web site listed first. The Business Secure Router counts each page viewed in a Web site as another hit on the Web site.
Hits	This column lists how many times each Web site has been visited. The count starts over at 0 if a Web site passes the hit count limit.

Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list to have the Business Secure Router record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 154 Protocol/Port report example

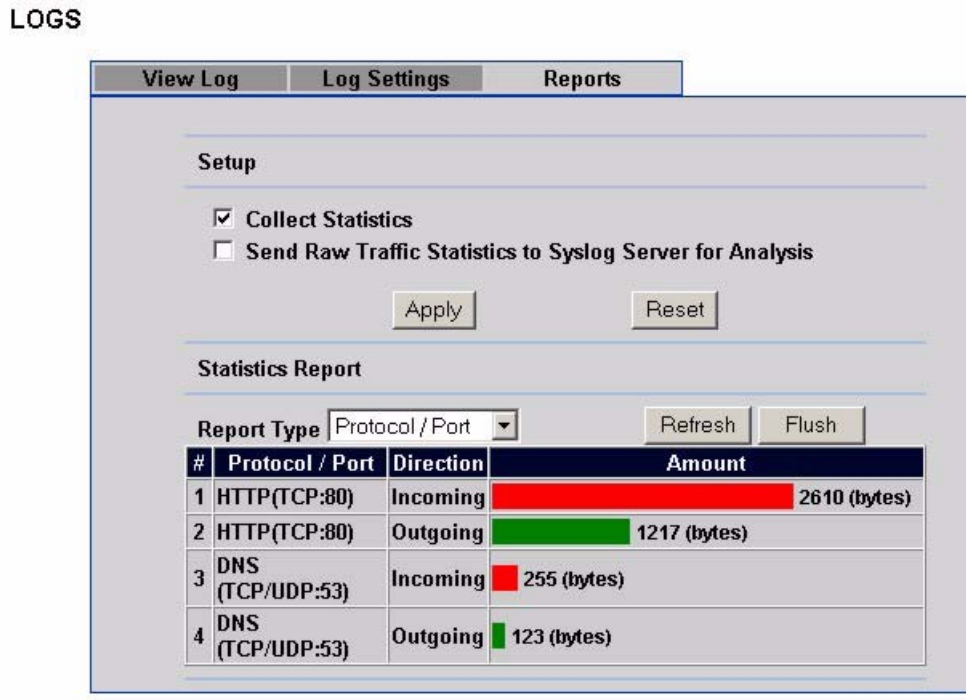


Table 105 describes the fields in Figure 154.

Table 105 Protocol/ Port Report

Label	Description
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the Business Secure Router. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This column lists the direction of travel of the traffic belonging to each protocol or service port listed. **Incoming** refers to traffic that is coming into the Business Secure Router's LAN from the WAN. **Outgoing** refers to traffic that is going out from the Business Secure Router's LAN to the WAN.
Amount	This column lists how much traffic has been sent and received for each protocol or service port. The measurement unit shown (bytes, Kilobytes, Megabytes or Gigabytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 107 on page 383).

Viewing LAN IP address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list to have the Business Secure Router record and display the LAN IP addresses that the most traffic has been sent to and from and how much traffic has been sent to and from those IP addresses.

Note: Computers take turns using dynamically assigned LAN IP addresses. The Business Secure Router continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

Figure 155 LAN IP address report example

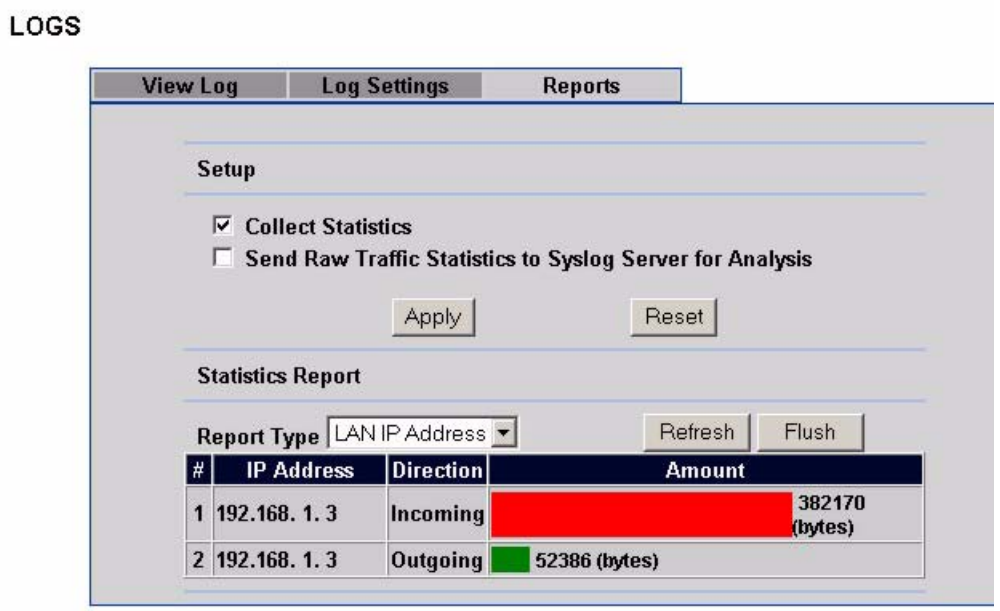


Table 106 describes the fields in Figure 155.

Table 106 LAN IP Address Report

Label	Description
IP Address	This column lists the LAN IP addresses to and from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and from which the most traffic was sent listed first.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kilobytes, Megabytes or Gigabytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see Table 107 on page 383).

Reports specifications

Table 107 lists detailed specifications on the reports feature.

Table 107 Report Specifications

Label	Description
Number of Web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per Web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

Chapter 21
Call scheduling screens

With call scheduling (applicable for PPPoA or PPPoE encapsulation only), you can dictate when a remote node is to be called and for how long.

Call scheduling introduction

Using the call scheduling feature, the Business Secure Router can manage a remote node and dictate when a remote node is to be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). Apply schedule sets in the **WAN IP** screen or the **WAN Dial Backup** screen.

Lower numbered sets take precedence over higher numbered sets, thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3, and 4 are applied in the remote node, set 1 takes precedence over set 2, 3, and 4 as the Business Secure Router, by default, applies the lowest numbered set first. Set 2 takes precedence over sets 3 and 4, and so on.

You can design up to 12 schedule sets. You can apply up to four schedule sets for a remote node.

Call schedule summary

Click **CALL SCHEDULE** to open the **Call Schedule Summary** screen.

Figure 156 Call schedule summary

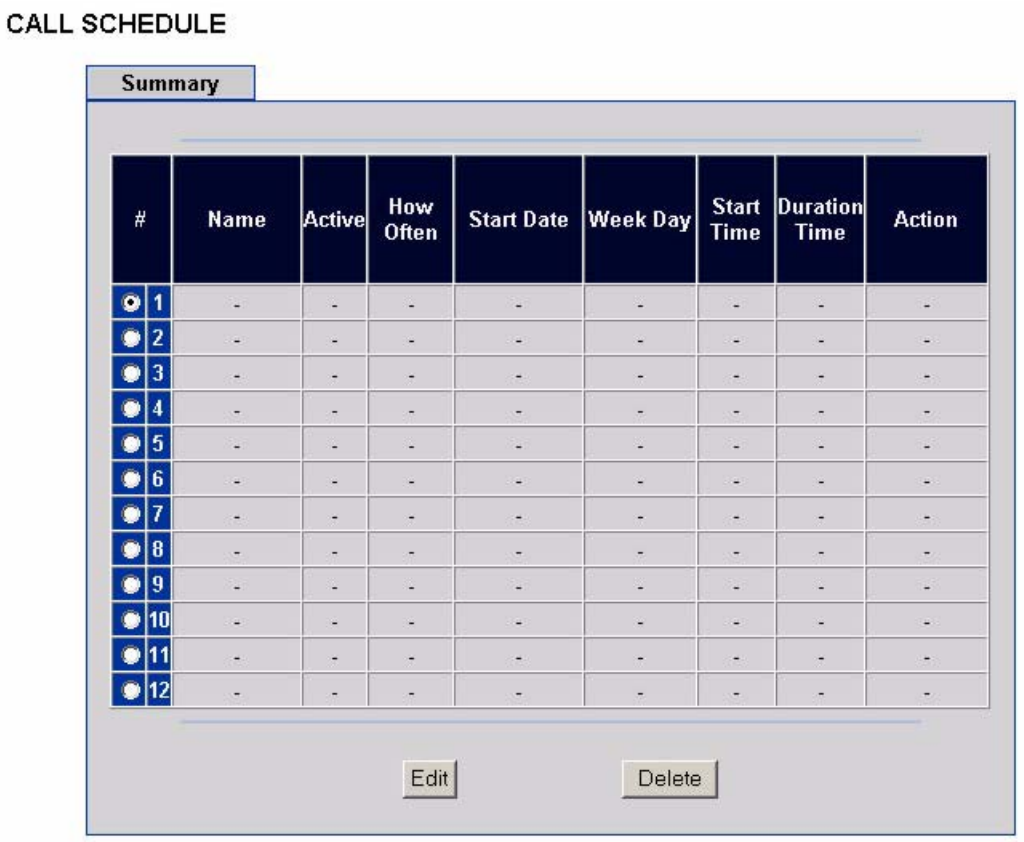

CALL SCHEDULE
Summary
Name Active How Often Start Date Week Day Start Time Duration Time Action
1 - - - - - - - -
2 - - - - - - - -
3 - - - - - - - -
4 - - - - - - - -
5 - - - - - - - -
6 - - - - - - - -
7 - - - - - - - -
8 - - - - - - - -
9 - - - - - - - -
10 - - - - - - - -
11 - - - - - - - -
12 - - - - - - - -
Edit
Delete

Table 108 describes the fields in Figure 156.

Table 108 Call Schedule Summary

Label	Description
#	This is the call schedule set number.
Name	This field displays the name of the call schedule set.
Active	This field shows whether the call schedule set is turned on (Yes) or off (No).
Start Date	This is the date (in year-month-day format) that the call schedule set takes effect.
Duration Date	This is the date (in year-month-day format) that the call schedule set ends.

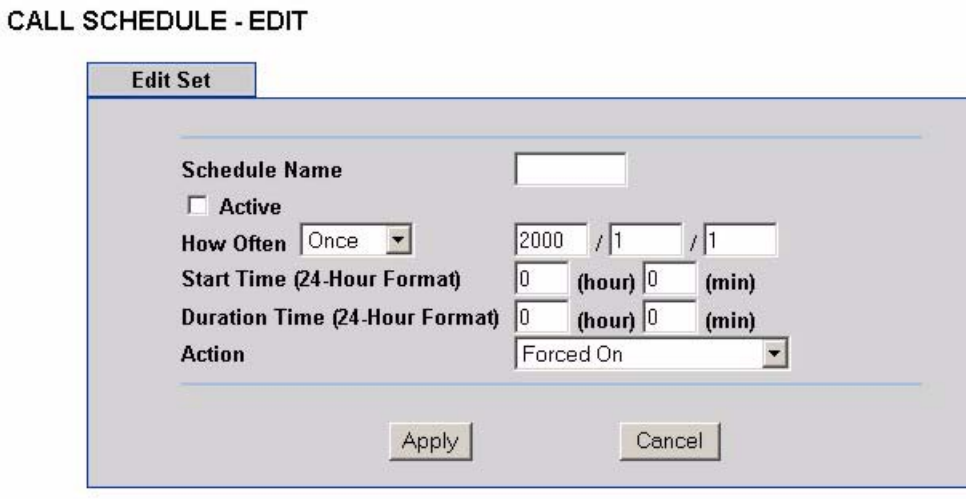
Table 108 Call Schedule Summary

Label	Description
Start Time	This is the time (in hour-minute format) when the schedule set takes effect.
Duration Time	This is the maximum length of time (in hour-minute format) that the schedule set applies the action displayed in the Action field.
Action	Forced On means that the connection is maintained whether or not there is a demand call on the line and persists for the time period specified in the Duration field. Forced Down means that the connection is blocked whether or not there is a demand call on the line. Enable Dial-On-Demand means that this schedule permits a demand call on the line. Disable Dial-On-Demand means that this schedule prevents a demand call on the line.
Edit	Click Edit to change a call schedule set.
Delete	Select the a call schedule set's radio button and click Delete to remove that call schedule set.

Call scheduling edit

To configure a schedule set, click the **Edit** button to display the screen shown in Figure 157.

Figure 157 Call schedule edit



If a connection has been already established, your Business Secure Router will not drop it. After the connection is dropped manually or it times out, that remote node can not be triggered again until the end of the **Duration**.

Table 109 Call schedule edit

Label	Description
Schedule Name	Enter a name (up to 16 characters) for the call schedule set. You can use numbers, the letters A-Z (upper or lower case) and the underscore (_) and @ symbols.
Active	Select this check box to turn on this call schedule set. Clear this check box to turn this call schedule set off.
Start Date	Set the date (in year-month-day format) when you want this call schedule set to take effect.
How Often	Select **Once** to use this schedule set only one time. Select **Weekly** to use this schedule every week. If you select **Once**, then enter the date the set will activate in year-month-day format. If you selected **Weekly** in the **How Often** field, then select the day or days of the week when the set will activate.
Start Time (24-Hour Format)	Enter the start time (in hour-minute format) when you want the schedule set to take effect.
Duration Time (24-Hour Format)	Enter the maximum length of time (in hour-minute format) that the schedule set is to apply the action configured in the Action field. The limit is 24 hours.
Action	Select an action for the schedule set to take. **Forced On** means that the connection is maintained whether or not there is a demand call on the line and persists for the time period specified in the Duration field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
Apply	Click **Apply** to save your changes to the Business Secure Router.
Cancel	Click **Cancel** to exit this screen without saving.

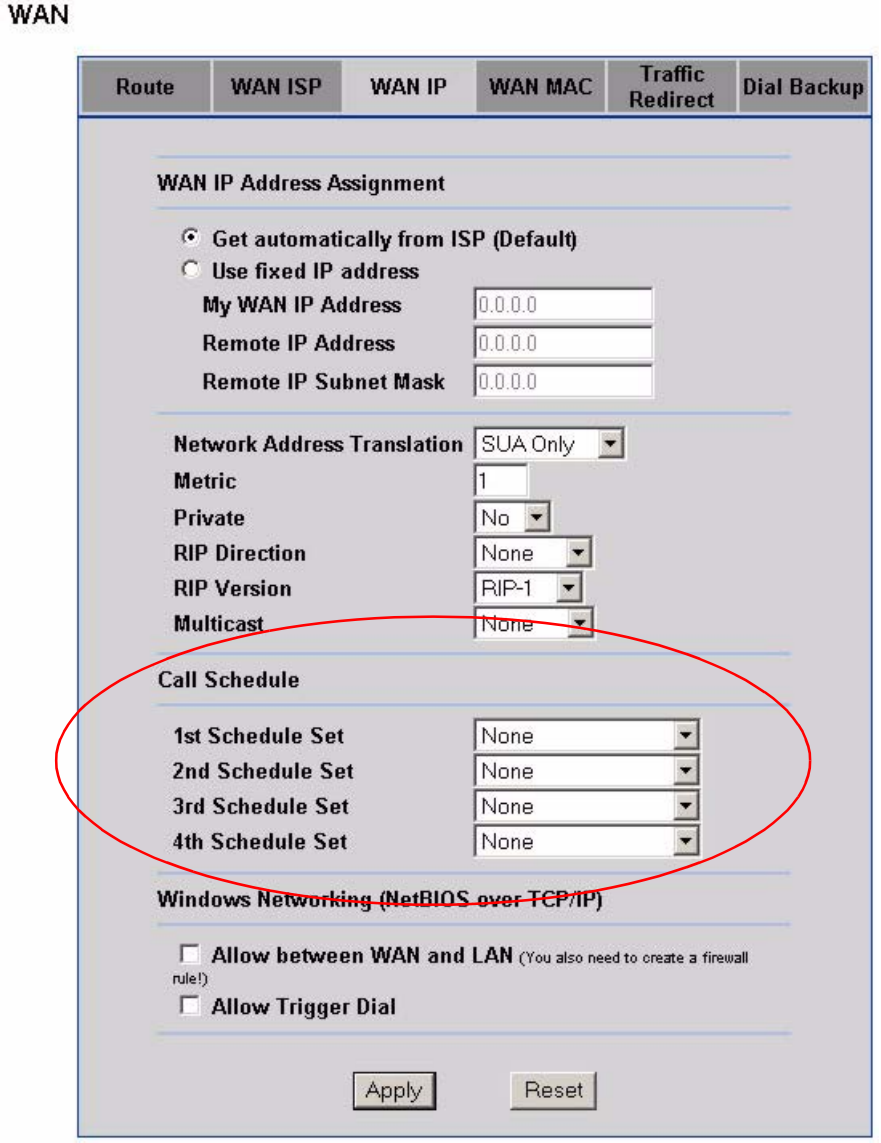
Applying Schedule Sets to a remote node

Once your schedule sets are configured, you must then apply them to the remote node. You can apply schedule sets when the Business Secure Router is set to use PPPoE or PPTP encapsulation (refer to “Configuring WAN ISP” on page 107).

Click **WAN**, **WAN IP** to display the **WAN IP** screen as shown in Figure 158. Use the screen to apply up to four schedule sets.

Figure 158 Applying Schedule Sets to a remote node

WAN



Chapter 22
Maintenance

This chapter displays system information such as firmware, port IP addresses, and port traffic statistics.

Maintenance overview

The maintenance screens can help you view system information, upload new firmware, manage configuration, and restart your Business Secure Router.

Status screen

Click **MAINTENANCE** to open the **Status** screen, where you can monitor your Business Secure Router. Note that these fields are READ-ONLY and only used for diagnostic purposes.

Figure 159 System Status

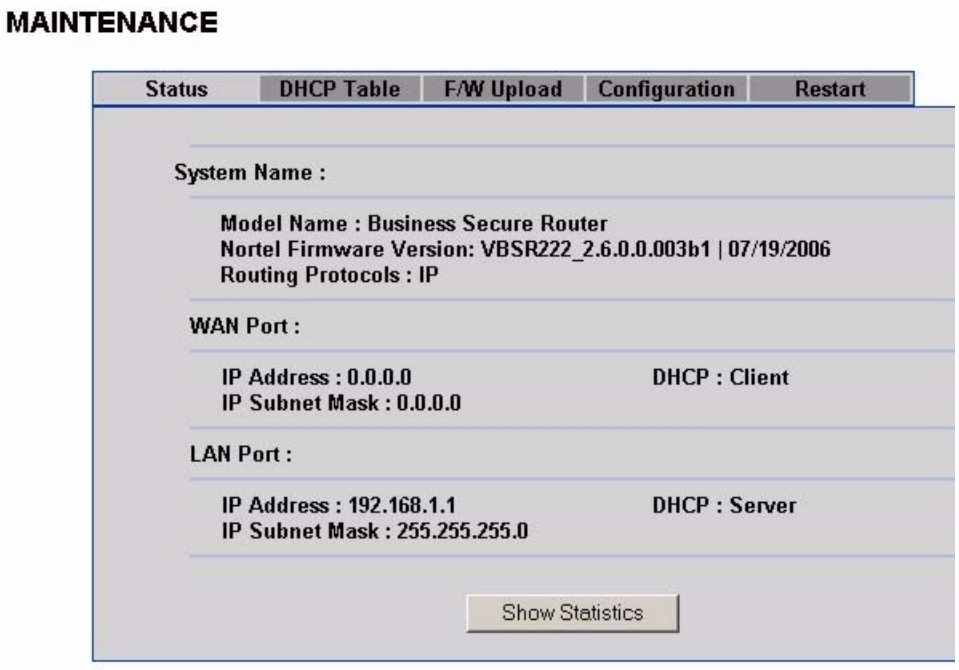


Table 110 describes the fields in Figure 159.

Table 110 System Status

Label	Description
System Name	This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name is also on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name.
Nortel Firmware Version:	The release of firmware currently on the Business Secure Router and the date the release was created.
Routing Protocols	This shows the routing protocol-**IP** for which the Business Secure Router is configured.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role-**Client** or **None**.

Table 110 System Status

Label	Description
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role–**Server** or **None**.

System statistics

Read-only information here includes port status and packet specific statistics. Also provided are system up time and poll intervals. The **Poll Interval(s)** field is configurable.

Figure 160 System Status: Show statistics

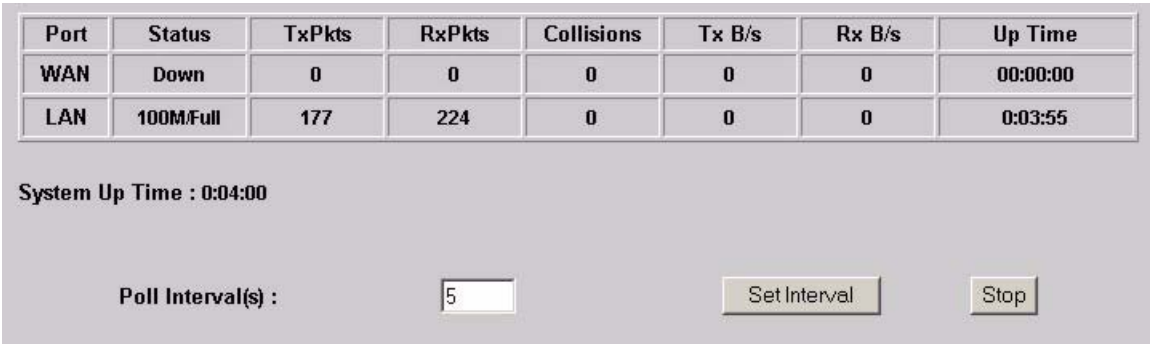


Table 111 describes the fields in Figure 160.

Table 111 System Status: Show statistics

Label	Description
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you are using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you are using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.

Table 111 System Status: Show statistics

Label	Description
Tx B/s	This displays the transmission speed, in bytes per second, on this port.
Rx B/s	This displays the reception speed, in bytes per second, on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the Business Secure Router has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics, click **Stop**.

DHCP Table screen

With DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) individual clients can obtain TCP/IP configuration at start-up from a server. You can configure the Business Secure Router as a DHCP server or disable it. When configured as a server, the Business Secure Router provides the TCP/IP configuration for the clients. If set to **None**, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computer must be configured manually.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name,** and **MAC Address**) of all network clients using the DHCP server.

Figure 161 DHCP Table

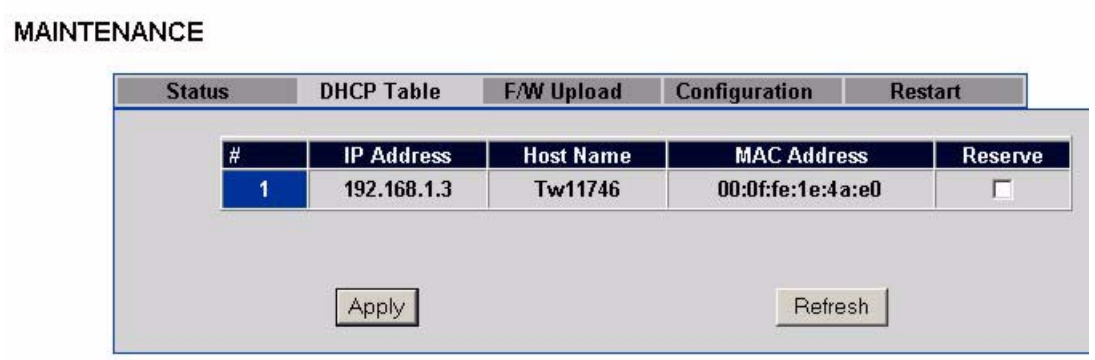


Table 112 describes the fields in Figure 161.

Table 112 DHCP Table

Label	Description
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select an entry's check box to have the Business Secure Router always assign the selected entries IP addresses to the corresponding MAC addresses (and host names). After you click **Apply**, the MAC address and IP address also display in the **LAN Static DHCP** screen (where you can edit them).
Refresh	Click **Refresh** to renew the screen.

F/W Upload screen

Find firmware at www.nortel.com/index.html in a file that usually uses the system model name with a *.bin extension. The upload process uses FTP (File Transfer Protocol) and can take up to two minutes. After a successful upload, the system reboots.

Click **MAINTENANCE**, and then the **F/W UPLOAD** tab. Follow the instructions to upload firmware to your Business Secure Router.

Figure 162 Firmware upload

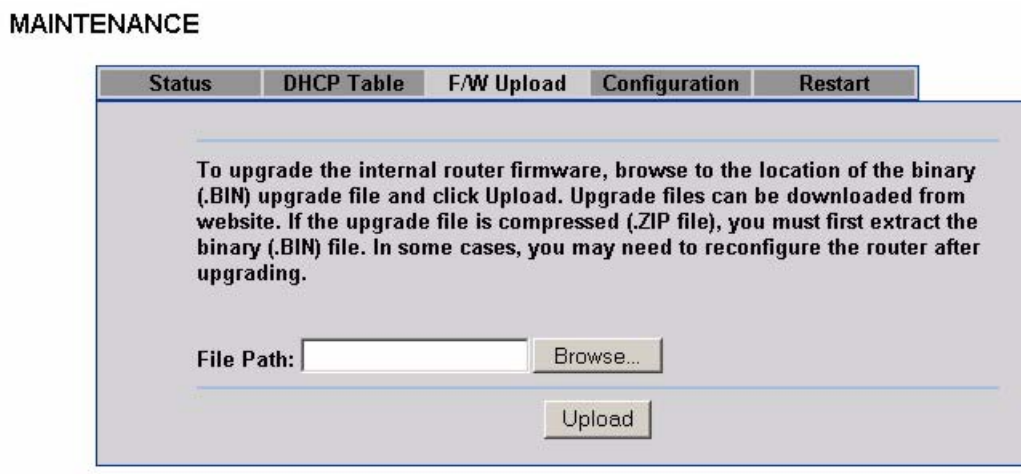

MAINTENANCE
Status
DHCP Table
F/W Upload
Configuration
Restart
To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.
File Path:
Browse...
Upload

Table 113 describes the fields in Figure 162.

Table 113 Firmware Upload

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process can take up to two minutes.

Note: Do not turn off the device while firmware upload is in progress!

After you see the **Firmware Upload in Process** (Figure 163) screen, wait two minutes before logging on to the device again.

Figure 163 Firmware Upload In Process

Firmware Upload In Progress
Warning!
Do Not Turn Off the Device.
Please wait for the device to finish restarting. This should take about two minutes.
To access the device after a successful firmware upload, you need to log in again. Check you new firmware version in the system status screen.

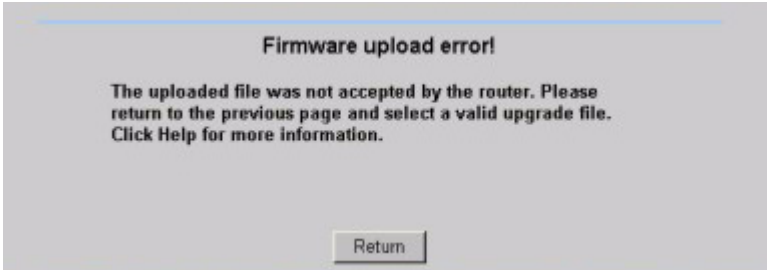
The device automatically restarts in this time, causing a temporary network disconnect. In some operating systems, you can see the icon Shown in Figure 164 on your desktop.

Figure 164 Network Temporarily Disconnected

After two minutes, log on again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the screen shown in Figure 165 appears. Uploading the wrong firmware file or a corrupted firmware file can cause this error. Click **Return** to return to the **F/W Upload** screen.

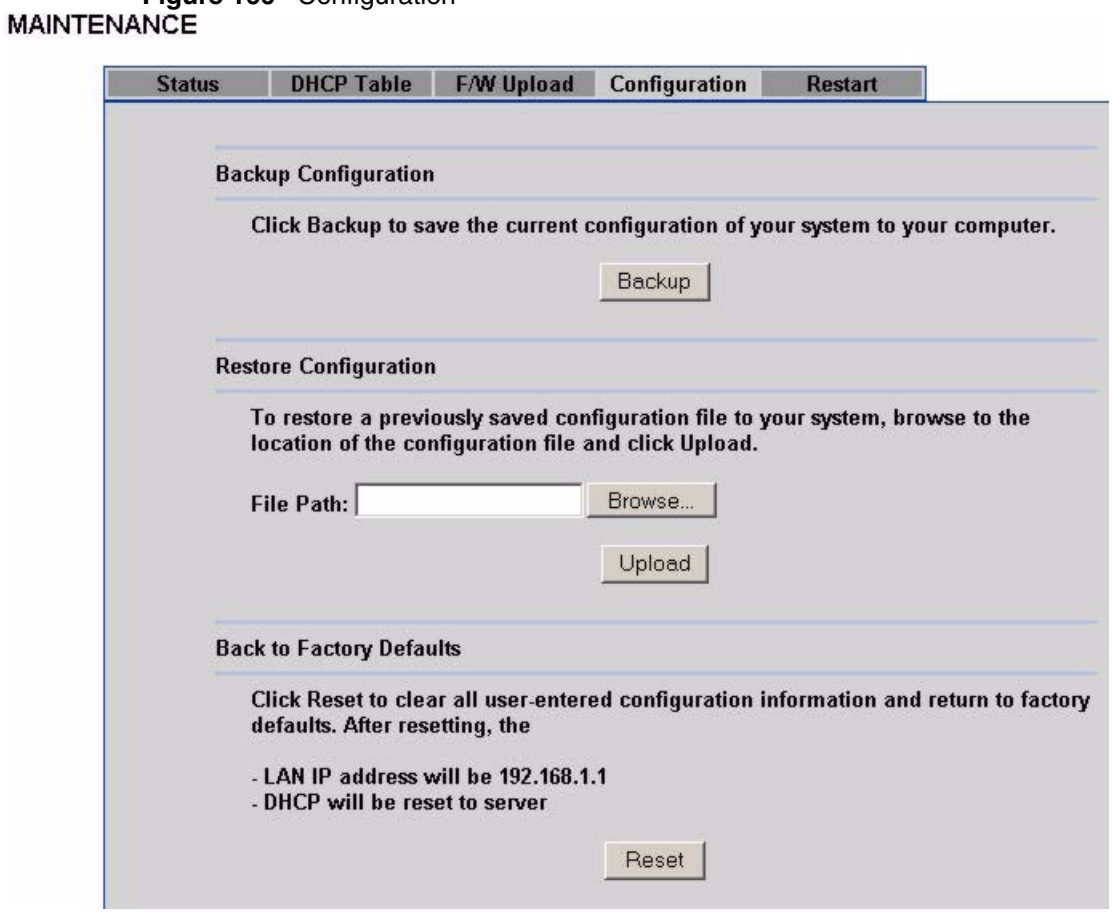
Figure 165 Firmware upload error


Firmware upload error!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

Configuration screen

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown in Figure 166.

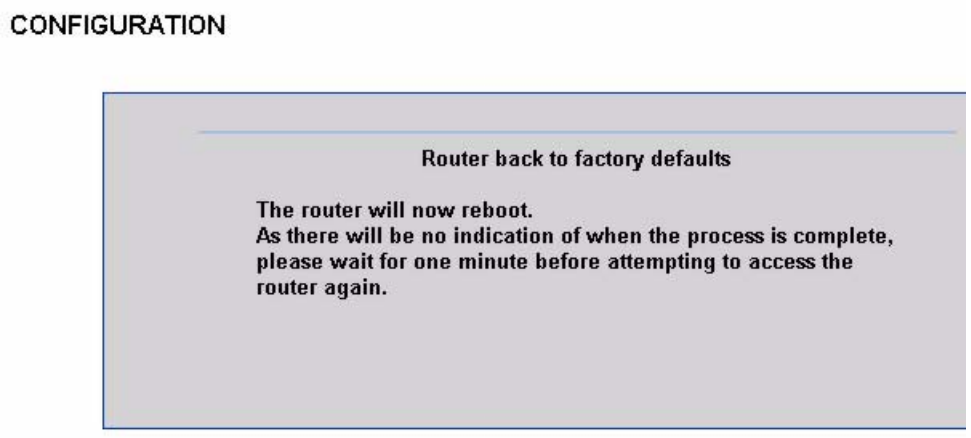
Figure 166 Configuration


MAINTENANCE
Status
DHCP Table
F/W Upload
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the Business Secure Router to its factory defaults. The warning screen appears (see Figure 167).

Figure 167 Reset warning message


CONFIGURATION
Router back to factory defaults
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Business Secure Router.

The Business Secure Router's LAN IP address changes back to 192.168.1.1 and the password reverts to "PlsChgMe!".

Backup configuration

With backup configuration, you can back up and save the device's current configuration to a 104 KB file on your computer. After your device is configured and functioning properly, Nortel recommends that you back up your configuration file before making configuration changes. The backup configuration file is useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

Restore configuration

With restore configuration, you can upload a new or previously saved configuration file from your computer to your Business Secure Router.

Table 114 Restore configuration

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the device while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging on to the device again.

Figure 168 Configuration Upload Successful

RESTORE CONFIGURATION
Restore Configuration Successful
The Router Is Rebooting Now.
Please Wait ...
After the device finishes rebooting, the login screen displays.

The device automatically restarts in this time, causing a temporary network disconnect. In some operating systems, you see the icon shown in Figure 169 on your desktop.

Figure 169 Network Temporarily Disconnected

If you uploaded the default configuration file, you need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301) guide for details about how to set up your computer's IP address.

If the upload was not successful, click **Return** to return to the **Configuration** screen.

Restart screen

With system restart, you can reboot the Business Secure Router without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the Business Secure Router reboot. This does not affect the Business Secure Router's configuration.

Figure 170 Restart screen

MAINTENANCE
Status
DHCP Table
F/W Upload
Configuration
Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

Appendix A Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Problems Starting Up the Business Secure Router

Table 115 Troubleshooting the Start-Up of your Business Secure Router

Problem	Corrective Action
None of the LEDs turn on when I turn on the Business Secure Router.	Make sure that the Business Secure Router's power adapter is connected to the Business Secure Router and plugged in to an appropriate power source. Check that the Business Secure Router and the power source are both turned on. Turn the Business Secure Router off and on. If the error persists, you likely have a hardware problem. In this case, contact your vendor.
I cannot access the Business Secure Router via the console port.	1. Make sure the Business Secure Router is connected to your computer's serial port.
	2. Make sure the communications program is configured correctly. Configure the communications software as follows: • VT100 terminal emulation • 9 600 b/s is the default speed on leaving the factory. Try other speeds in case the speed has been changed. • No parity, 8 data bits, 1 stop bit, data flow set to none.

Problems with the LAN LED

Table 116 Troubleshooting the LAN LED

Problem	Corrective Action
The LAN LEDs do not turn on.	Check your Ethernet cable connections.
	Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.

Problems with the LAN interface

Table 117 Troubleshooting the LAN Interface

Problem	Corrective Action
I cannot access the Business Secure Router from the LAN.	Check your Ethernet cable type and connections. Refer to the *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301) guide for LAN connection instructions.
	Make sure the computer's Ethernet adapter is installed and functioning properly.
I cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. If they are all off, check the cables between your Business Secure Router and hub or the computer.
	Verify that the IP address and the subnet mask of the Business Secure Router and the computers are on the same subnet.

Problems with the WAN interface

Table 118 Troubleshooting the WAN Interface

Problem	Corrective Action
Cannot get WAN IP address from the ISP.	Refer to the *Nortel Business Secure Router 222 — Fundamentals* (NN47922-301) guide for initial set up of the Business Secure Router.The ISP provides the WAN IP address after authentication. Authentication can be through the username and password, the MAC address, or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a username and password if you are using PPPoE or PPTP encapsulation. Make sure that you have entered the correct Service Type, Username and Password (the username and password are case-sensitive). Use the WAN screens in the WebGUI.
	If your ISP requires MAC address authentication, clone the MAC address from your computer on the LAN as the Business Secure Router's WAN MAC address. Use the WAN screens in the WebGUI. Nortel recommends that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication.
	If your ISP requires host name authentication, configure your computer's name as the Business Secure Router's system name (use the WebGUI's wizard or **System General** screen to configure the system name).

Problems with Internet Access

Table 119 Troubleshooting Internet Access

Problem	Corrective Action
Cannot access the Internet.	Connect your cable or DSL modem with the Business Secure Router using the appropriate cable.Check with the manufacturer of your cable or DSL device about your cable requirement because some devices require crossover cable and others a regular straight-through cable.
	Verify your settings in the WAN screens.
Internet connection disconnects.	Check the call scheduling rules.
	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in the WAN screens.
	Contact your ISP.

Problems accessing an internet Web site

Table 120 Troubleshooting Web Site Internet Access

Problem	Corrective Action
Cannot connect to a Web site on the Internet.	Disable content filtering and clear your browser cache. Try connecting to the Web site again. If you can now connect to this site, the content filter blocked original access. Check your content filter settings if this was not your intention.
	If you cannot connect to the site even after you disable content filtering, check your device connections and Internet access settings. Your username and password can be case-sensitive. If device connections and Internet access settings are correct, contact your ISP.

Problems with the password

Table 121 Troubleshooting the password

Problem	Corrective Action
I cannot access the Business Secure Router.	The administrator username is “nnadmin”. The default password is “PlsChgMe!”. The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you must reset the Business Secure Router to the default configuration file. This restores all of the factory defaults, including the password. Press the rear panel **RESET** button for longer than three seconds to return the Business Secure Router to the factory defaults.

Problems with the WebGUI

Table 122 Troubleshooting the WebGUI

Problem	Corrective Action
I cannot access the WebGUI.	Make sure that there is not an SMT console session running.
	Check that you have enabled Web service access. If you have configured a remote management secured client IP address, your computer's IP address must match it.
	For WAN access, you must configure remote management to allow server access from the Wan (or all). You must also configure a firewall rule to allow access from the WAN.
	Your computer's and the Business Secure Router's IP addresses must be on the same subnet for LAN access.
	If you changed the Business Secure Router's LAN IP address, then enter the new one as the URL.
	Remove any filters in SMT menu 3.1 (LAN) or menu 11.1.4 (WAN) that block Web service.

Problems with Remote Management

Table 123 Troubleshooting Remote Management

Problem	Corrective Action
I cannot remotely manage the Business Secure Router from the LAN or the WAN.	Check your remote management and firewall configuration.
	Use the Business Secure Router's WAN IP address when configuring from the WAN. Use the Business Secure Router's LAN IP address when configuring from the LAN.
	Refer to "Problems with the LAN interface" on page 404 for instructions about checking your LAN connection.
	Refer to the "Problems with the WAN interface" on page 405 for instructions about checking your WAN connection.
	See also "Problems with the WebGUI" on page 407.

Allowing Pop-up Windows, JavaScript and Java Permissions

In order to use the WebGUI, you must allow:

- Web browser pop-up windows from your device
- JavaScript
- Java permissions

Internet Explorer Pop-up Blockers

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions vary

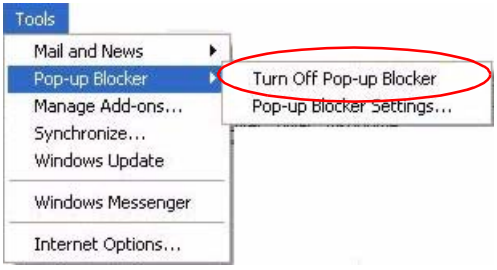
Disable pop-up blocking to log on to your device, if necessary.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or enable pop-up blocking and create an exception for your device's IP address.

Allowing Pop-ups

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 171 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen.

Figure 172 Internet Options

3 Click **Apply** to save this setting.

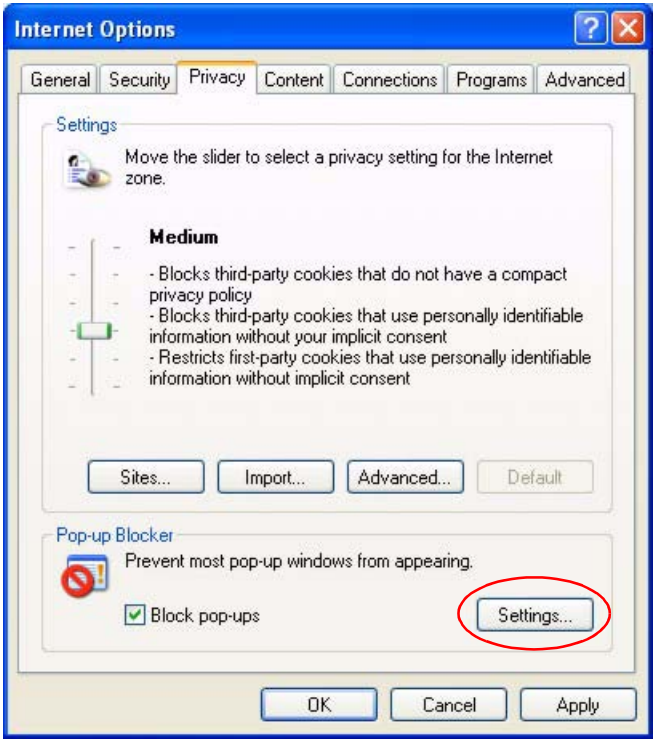
Enabling Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…** to open the **Pop-up Blocker Settings** screen.

Figure 173 Internet options



3 Type the IP address of your device (the Web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 174 Pop-up Blocker settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Internet Options** screen.

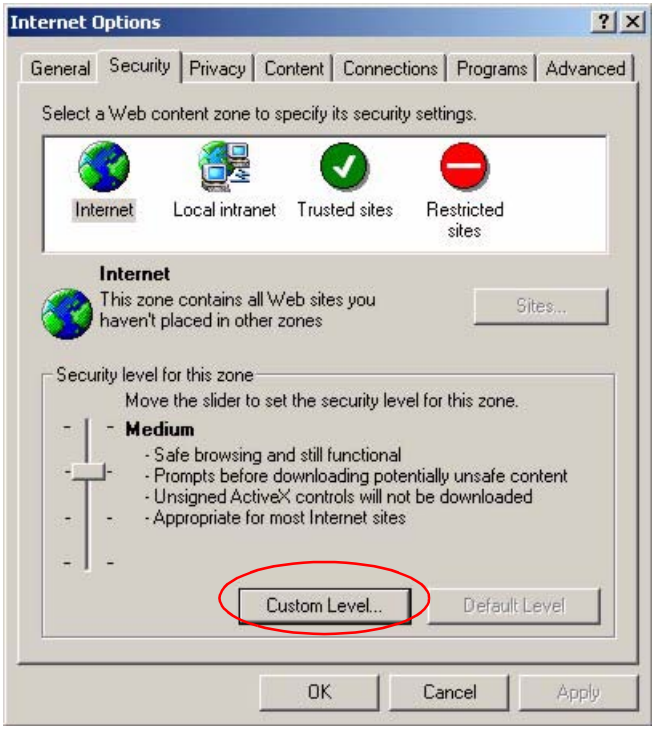
6 Click **Apply** to save this setting.

Internet Explorer JavaScript

If pages of the WebGUI do not display properly in Internet Explorer, check that JavaScript and Java permissions are enabled.

1 In Internet Explorer, click **Tools**, **Internet Options,** and then the **Security** tab.

Figure 175 Internet options



2 Click the **Custom Level...** button.

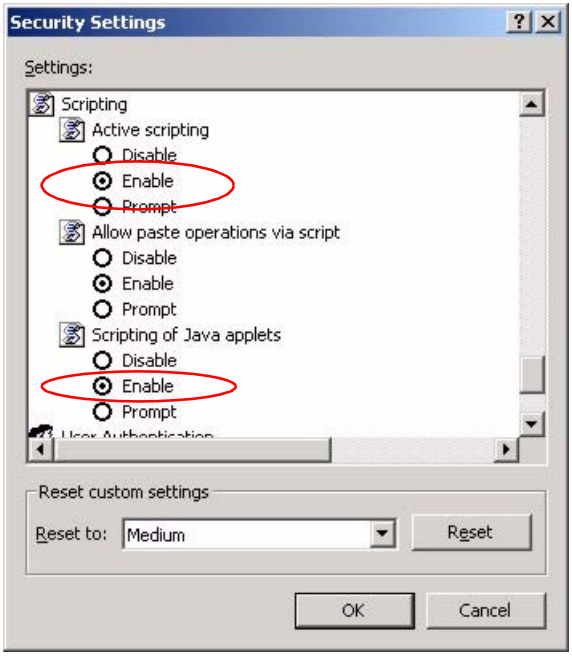
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 176 Security Settings - Java Scripting



Internet Explorer Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options,** and then the **Security** tab.

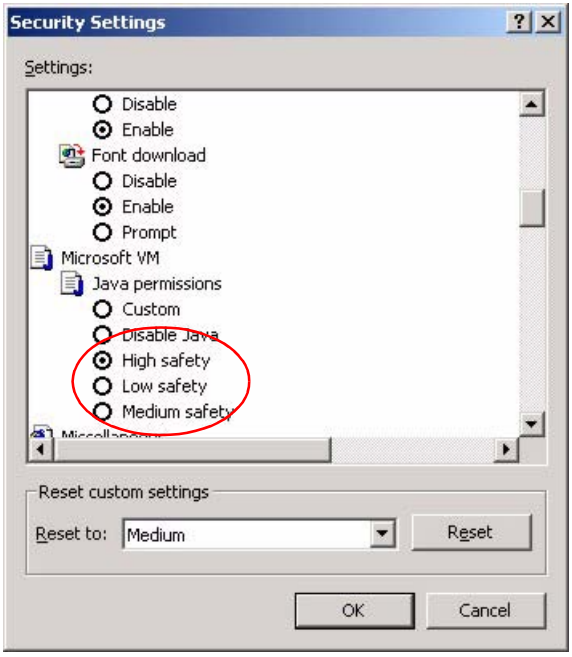
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 177 Security Settings - Java



JAVA (Sun)

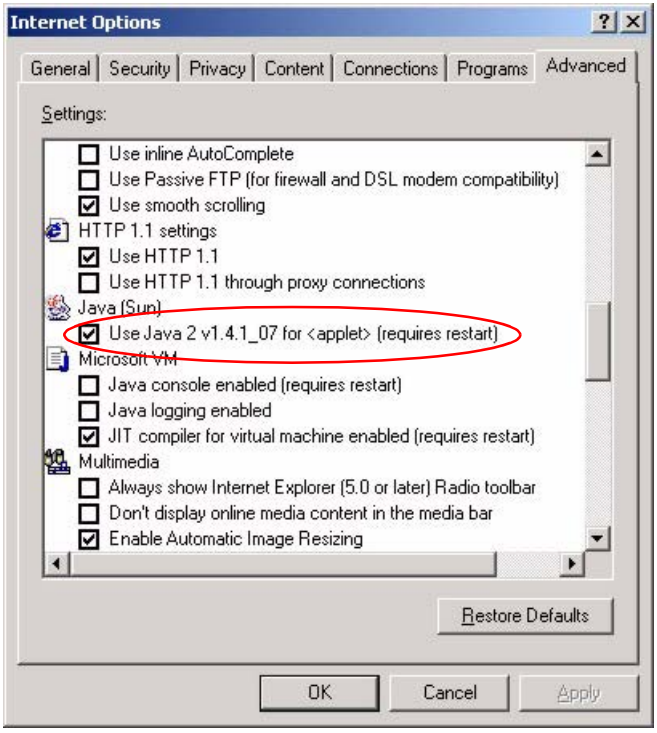
1 From Internet Explorer, click **Tools**, **Internet Options,** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

4 Close your existing browser session and open a new browser.

Figure 178 Java (Sun)



Netscape Pop-up Blockers

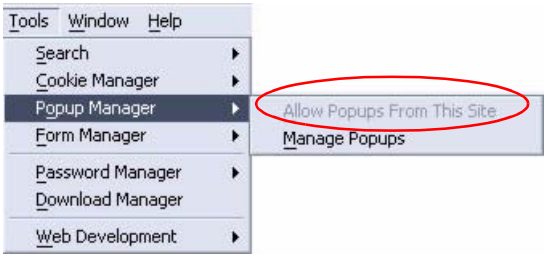
Note: Netscape 7.2 screens are used here. Screens for other Netscape versions vary

Either disable the blocking of unrequested pop-up windows (enabled by default in Netscape) or allow pop-ups from Web sites by creating an exception for your device's IP address.

Allowing Pop-ups

1 In Netscape, click **Tools**, **Popup Manager** and then select **Allow Popups From This Site**.

Figure 179 Allow Popups from this site



2 In the Netscape search toolbar, you can enable and disable pop-up blockers for Web sites.

Figure 180 Netscape Search Toolbar

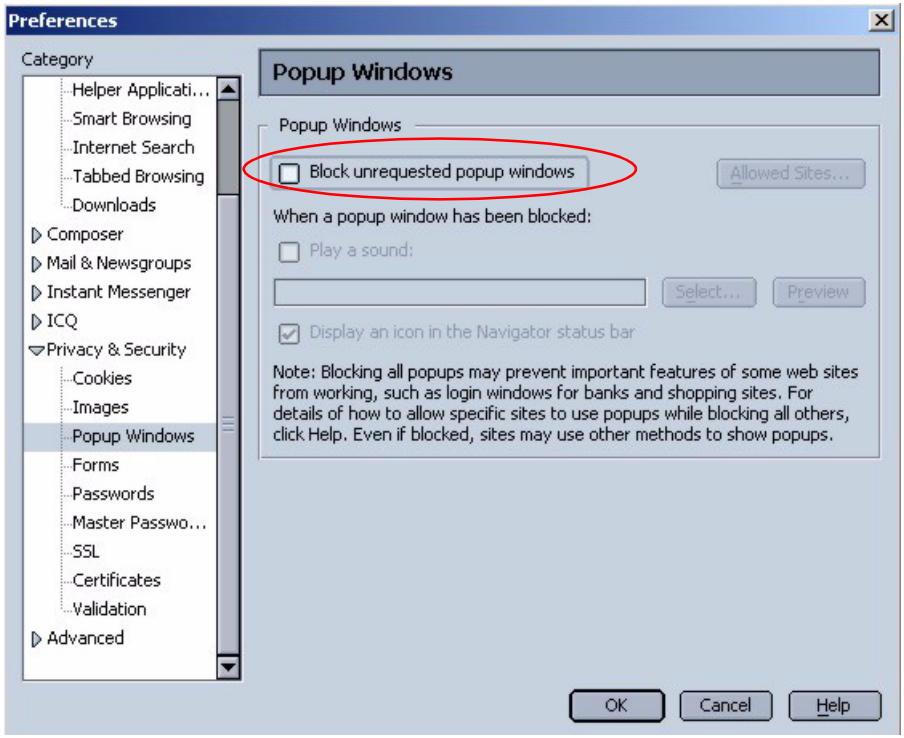
You can also check if pop-up blocking is disabled in the **Popup Windows** screen in the **Privacy & Security** directory.

1 In Netscape, click **Edit** and then **Preferences**.

2 Click the **Privacy & Security** directory and then select **Popup Windows**.

3 Clear the **Block unrequested popup windows** check box.

Figure 181 Popup Windows



4 Click **OK** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, follow these steps:

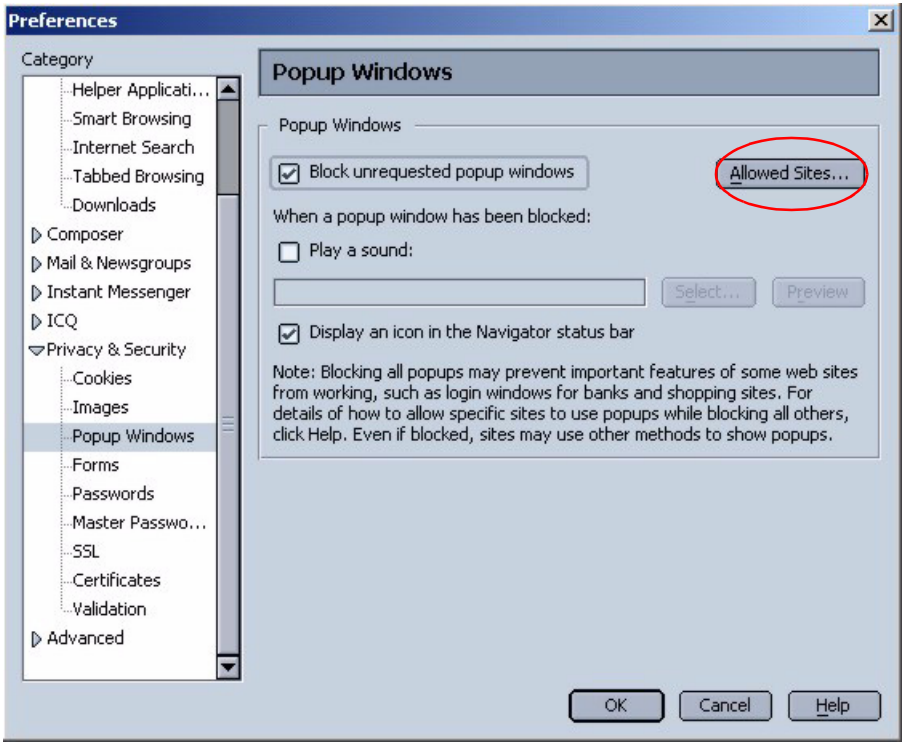
1 In Netscape, click **Edit,** and then **Preferences**.

2 In the **Privacy & Security** directory, select **Popup Windows**.

3 Make sure the **Block unrequested popup windows** check box is selected.

4 Click the **Allowed Sites...** button.

Figure 182 Popup Windows



5 Type the IP address of your device (the Web page that you do not want to have blocked) with the prefix http://. For example, http://192.168.1.1.

6 Click **Add** to move the IP address to the **Site** list.

Figure 183 Allowed Sites

7 Click **OK** to return to the **Popup Windows** screen.

8 Click **OK** to save this setting.

Netscape Java Permissions and JavaScript

If pages of the WebGUI do not display properly in Netscape, check that JavaScript and Java permissions are enabled.

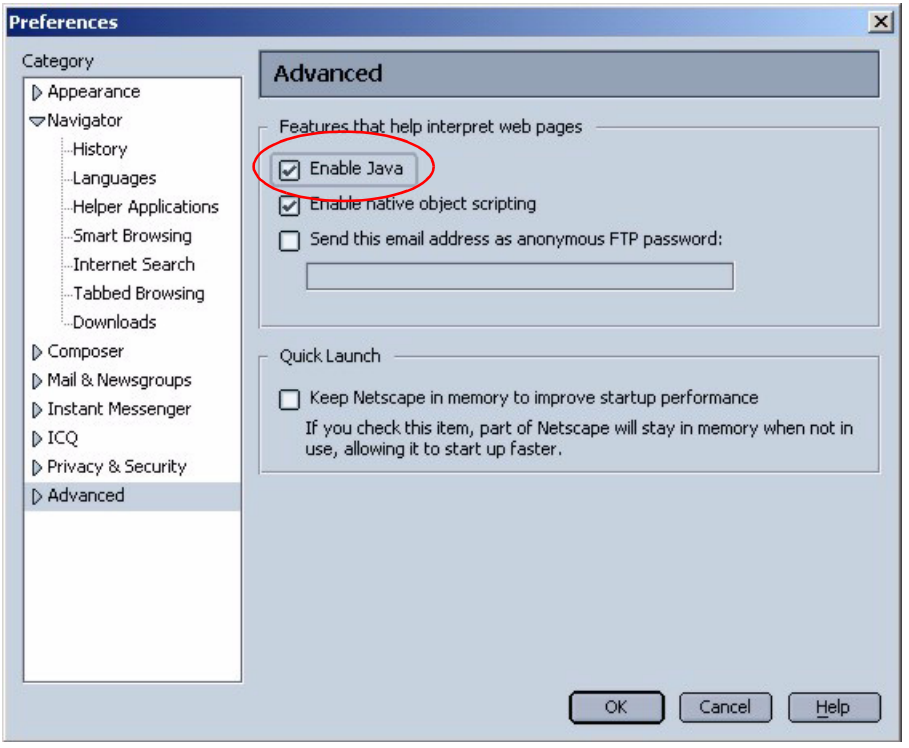
1 In Netscape, click **Edit** and then **Preferences**.

2 Click the **Advanced** directory.

3 In the **Advanced** screen, make sure the **Enable Java** check box is selected.

4 Click **OK** to close the window.

Figure 184 Advanced

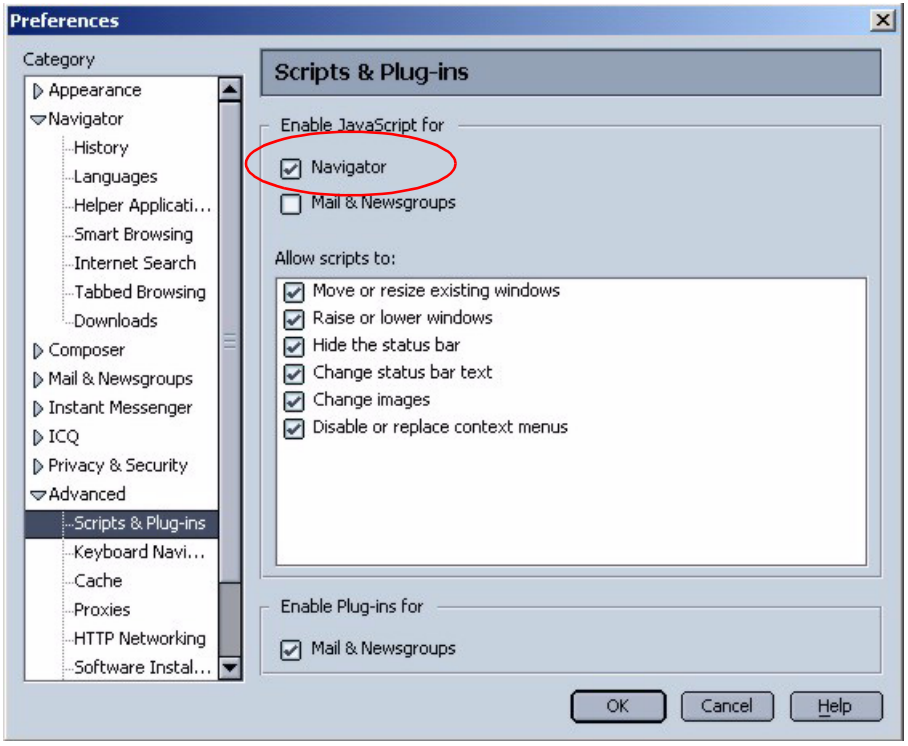


5 Click the **Advanced** directory and then select **Scripts & Plug-ins**.

6 Make sure the **Navigator** check box is selected in the enable JavaScript section.

7 Click **OK** to close the window.

Figure 185 Scripts & Plug-ins



Appendix B
Log Descriptions

This appendix provides descriptions of example log messages.

Table 124 System Error Logs

Log Message	Description
`%s exceeds the max. number of session per host!`	This attempt to create a SUA/NAT session exceeds the maximum number of SUA/NAT session table entries allowed to be created per host.

Table 125 System Maintenance Logs

Log Message	Description
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's WebGUI interface.
`WEB Login Fail`	Someone has failed to log on to the router's WebGUI interface.
`TELNET Login Successfully`	Someone has logged on to the router via Telnet.

Table 125 System Maintenance Logs

Log Message	Description
TELNET Login Fail	Someone has failed to log on to the router via Telnet.
FTP Login Successfully	Someone has logged on to the router via FTP.
FTP Login Fail	Someone has failed to log on to the router via FTP.
NAT Session Table is Full!	The maximum number of SUA/NAT session table entries has been exceeded and the table is full.

Table 126 UPnP Logs

Log Message	Description
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 127 Content Filtering Logs

Category	Log Message	Description
URLFOR	IP/Domain Name	The Business Secure Router allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	IP/Domain Name	The Business Secure Router blocked access to this IP address or domain name due to a forbidden keyword. All Web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
JAVBLK	IP/Domain Name	The Business Secure Router blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Table 128 Attack Logs

Log Message	Description
attack TCP	The firewall detected a TCP attack.
attack UDP	The firewall detected an UDP attack.
attack IGMP	The firewall detected an IGMP attack.

Table 128 Attack Logs

Log Message	Description
attack ESP	The firewall detected an ESP attack.
attack GRE	The firewall detected a GRE attack.
attack OSPF	The firewall detected an OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack; see the section about ICMP messages for type and code details.
land TCP	The firewall detected a TCP land attack.
land UDP	The firewall detected an UDP land attack.
land IGMP	The firewall detected an IGMP land attack.
land ESP	The firewall detected an ESP land attack.
land GRE	The firewall detected a GRE land attack.
land OSPF	The firewall detected an OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack; see the section about ICMP messages for type and code details.
ip spoofing - WAN TCP	The firewall detected a TCP IP spoofing attack on the WAN port.
ip spoofing - WAN UDP	The firewall detected an UDP IP spoofing attack on the WAN port.
ip spoofing - WAN IGMP	The firewall detected an IGMP IP spoofing attack on the WAN port.
ip spoofing - WAN ESP	The firewall detected an ESP IP spoofing attack on the WAN port.
ip spoofing - WAN GRE	The firewall detected a GRE IP spoofing attack on the WAN port.
ip spoofing - WAN OSPF	The firewall detected an OSPF IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.

Table 128 Attack Logs

Log Message	Description
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry TCP`	The firewall detected a TCP IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry UDP`	The firewall detected an UDP IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry IGMP`	The firewall detected an IGMP IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry ESP`	The firewall detected an ESP IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry GRE`	The firewall detected a GRE IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry OSPF`	The firewall detected an OSPF IP spoofing attack while the Business Secure Router did not have a default route.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack while the Business Secure Router did not have a default route.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack.

For type and code details, see Table 131.

Table 129 Access Logs

Log Message	Description
`Firewall default policy: TCP (set:%d)`	TCP access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: UDP (set:%d)`	UDP access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.

Table 129 Access Logs

Log Message	Description
`Firewall default policy: ICMP (set:%d, type:%d, code:%d)`	ICMP access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: IGMP (set:%d)`	IGMP access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: ESP (set:%d)`	ESP access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: GRE (set:%d)`	GRE access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: OSPF (set:%d)`	OSPF access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: (set:%d)`	Access matched the default policy of the listed ACL set and the Business Secure Router blocked or forwarded it according to the ACL set's configuration.
`Firewall rule match: TCP (set:%d, rule:%d)`	TCP access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: UDP (set:%d, rule:%d)`	UDP access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: IGMP (set:%d, rule:%d)`	IGMP access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: ESP (set:%d, rule:%d)`	ESP access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: GRE (set:%d, rule:%d)`	GRE access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule match: OSPF (set:%d, rule:%d)`	OSPF access matched the listed a firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.

Table 129 Access Logs

Log Message	Description
`Firewall rule match: (set:%d, rule:%d)`	Access matched the listed firewall rule and the Business Secure Router blocked or forwarded it according to the rule's configuration.
`Firewall rule NOT match: TCP (set:%d, rule:%d)`	TCP access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: UDP (set:%d, rule:%d)`	UDP access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: IGMP (set:%d, rule:%d)`	IGMP access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: ESP (set:%d, rule:%d)`	ESP access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: GRE (set:%d, rule:%d)`	GRE ac access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: OSPF (set:%d, rule:%d)`	OSPF access did not match the listed firewall rule and the Business Secure Router logged it.
`Firewall rule NOT match: (set:%d, rule:%d)`	Access did not match the listed firewall rule and the Business Secure Router logged it.
`Filter default policy DROP!`	TCP access matched a default filter policy and the Business Secure Router dropped the packet to block access.
`Filter default policy DROP!`	UDP access matched a default filter policy and the Business Secure Router dropped the packet to block access.
`Filter default policy DROP!`	ICMP access matched a default filter policy and the Business Secure Router dropped the packet to block access.
`Filter default policy DROP!`	Access matched a default filter policy and the Business Secure Router dropped the packet to block access.

Table 129 Access Logs

Log Message	Description
`Filter default policy DROP!`	Access matched a default filter policy (denied LAN IP) and the Business Secure Router dropped the packet to block access.
`Filter default policy FORWARD!`	TCP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	UDP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet.
`Filter match DROP <set %d/rule %d>`	TCP access matched the listed filter rule and the Business Secure Router dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	UDP access matched the listed filter rule and the Business Secure Router dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	ICMP access matched the listed filter rule and the Business Secure Router dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule and the Business Secure Router dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP) and the Business Secure Router dropped the packet to block access.
`Filter match FORWARD <set %d/rule %d>`	TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet.

Table 129 Access Logs

Log Message	Description
`(set:%d)`	With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see Table 130). With filter messages, this is the number of the filter set.
`(rule:%d)`	With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set.With filter messages, this is the number of an individual filter rule.
`Router sent blocked web site message`	
`Triangle route packet forwarded`	The firewall allowed a triangle route session to pass through.
`Firewall sent TCP packet in response to DoS attack`	The firewall detected a DoS attack and sent a TCP packets in response.
`Firewall sent TCP reset packets`	The firewall sent out TCP reset packets.
`Packet without a NAT table entry blocked`	The router blocked a packet that did not have a corresponding SUA/NAT table entry.
`Out of order TCP handshake packet blocked`	The router blocked a TCP handshake packet that came out of the proper order.
`Drop unsupported/ out-of-order ICMP`	The Business Secure Router generates this log after it drops an ICMP packet due to one of the following two reasons: 1. The Business Secure Router does not support the ICMP packet's protocol. 2. The ICMP packet is an echo reply for which there was no corresponding echo request.
`Router sent ICMP response packet (type:%d, code:%d)`	The router sent an ICMP response packet. This packet automatically bypasses the firewall.

For type and code details, see Table 131.

Table 130 ACL Setting Notes

ACL Set Number	Direction	Description
1	LAN to WAN	ACL set 1 for packets traveling from the LAN to the WAN.
2	WAN to LAN	ACL set 2 for packets traveling from the WAN to the LAN.
7	LAN to LAN/Business Secure Router	ACL set 7 for packets traveling from the LAN to the LAN or the Business Secure Router.
8	WAN to WAN/Business Secure Router	ACL set 8 for packets traveling from the WAN to the WAN or the Business Secure Router.

Table 131 ICMP Notes

Type	Code	Description
0		Echo reply
	0	Echo reply message
3		Destination unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because the packet was set to Don't Fragment (DF)
	5	Source route failed
4		Source quench
	0	A gateway discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of service and network

Table 131 ICMP Notes

Type	Code	Description
	3	Redirect datagrams for the Type of service and host
8		Echo
	0	Echo message
11		Time exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp reply
	0	Timestamp reply message
15		Information request
	0	Information request message
16		Information reply
	0	Information reply message

Table 132 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>	This message is sent by the RAS when this syslog is generated. The messages and notes are defined in this appendix.

VPN/IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log, as shown in Figure 186, which shows a typical log from the initiator of a VPN connection.

Figure 186 Example VPN Initiator IPSec Log

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

VPN Responder IPSec Log

Figure 187 shows a typical log from the VPN connection peer.

Figure 187 Example VPN Responder IPSec Log

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

This menu is useful for troubleshooting your Business Secure Router. A log index number, the date and time the log was created, and a log message are displayed.

Note: Double exclamation marks (!!) denote an error or warning message.

Table 133 shows sample log messages during IKE key exchange.

Note: A PYLD_MALFORMED packet usually means that the two ends of the VPN tunnel are not using the same preshared key.

Table 133 Sample IKE Key Exchange Logs

Log Message	Description
`Send <Symbol> Mode request to <IP>Send <Symbol> Mode request to <IP>`	The Business Secure Router started negotiation with the peer.
`Recv <Symbol> Mode request from <IP>Recv <Symbol> Mode request from <IP>`	The Business Secure Router received an IKE negotiation request from the peer.
`Recv:<Symbol>`	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log (see Table 135).
`Phase 1 IKE SA process done`	Phase 1 negotiation finished.
`Start Phase 2: Quick Mode`	Phase 2 negotiation begins using Quick Mode.
`!! IKE Negotiation is in process`	The Business Secure Router has begun negotiation with the peer for the connection, but the IKE key exchange has not completed.
`!! Duplicate requests with the same cookie`	The Business Secure Router received multiple requests from the same peer but is still processing the first IKE packet from that peer.
`!! No proposal chosen`	The parameters configured for Phase 1 or Phase 2 negotiations do not match. Check all protocols and settings for these phases. For example, one party uses 3DES encryption, but the other party uses DES encryption, so the connection fails.
`!! Verifying Local ID failed!! Verifying Remote ID failed`	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, the connection fails.
`!! Local / remote IPs of incoming request conflict with rule <#d>`	If the security gateway is "0.0.0.0", the Business Secure Router uses the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule, the connection is not allowed.
`!! Invalid IP <IP start>/ <IP end>`	The peer's "Local IP Addr" range is invalid.

Table 133 Sample IKE Key Exchange Logs

Log Message	Description
`!! Remote IP <IP start> / <IP end> conflicts`	If the security gateway is "0.0.0.0", the Business Secure Router uses the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, the Business Secure Router does not accept VPN connection requests from this peer.
`!! Active connection allowed exceeded`	The Business Secure Router limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
`!! IKE Packet Retransmit`	The Business Secure Router did not receive a response from the peer and retransmits the last packet sent.
`!! Failed to send IKE Packet`	The Business Secure Router cannot send IKE packets due to a network error.
`!! Too many errors! Deleting SA`	The Business Secure Router deletes an SA when too many errors occur.
`!! Phase 1 ID type mismatch`	The ID type of an incoming packet does not match the local's peer ID type.
`!! Phase 1 ID content mismatch`	The ID content of an incoming packet does not match the local's peer ID content.
`!! No known phase 1 ID type found`	The ID type of an incoming packet does not match any known ID type.
`Peer ID: IP address type <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.
`vs. My Remote <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match.
`vs. My Local <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match.

Table 133 Sample IKE Key Exchange Logs

Log Message	Description
-> <symbol>	The router sent a payload type of IKE packet.
Error ID Info	The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range, or subnet) do not match. Check all protocols and settings for these phases.

Table 134 shows sample log messages during packet transmission.

Table 134 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the Business Secure Router's WAN IP changes, all configured My IP Addr change to 0.0.0.0. If this field is configured as 0.0.0.0, the Business Secure Router uses the current Business Secure Router WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find IPSec SA	The Business Secure Router cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Cannot find outbound SA for rule <%d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
!! Discard REPLAY packet	The Business Secure Router discards any packets received with the wrong sequence number.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the Business Secure Router drops the connection.

Table 135 shows RFC-2408 ISAKMP payload types that the log displays. Refer to the RFC for detailed information about each type.

Table 135 RFC-2408 ISAKMP Payload Types

Log Display	Payload Type
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Table 136 PKI Logs

Log Message	Description
`Enrollment successful`	The SCEP online certificate enrollment succeeded. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was succeeded. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.

Table 136 PKI Logs

Log Message	Description
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name did not pass the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. See Table 137 for the corresponding descriptions of the codes.

Table 137 Certificate Path Verification Failure Reason Codes

Code	Description
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 138 IEEE 802.1X Logs

Log Message	Description
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged off a user whose session expired.
User logout because of user deassociation.	The router logged off a user who ended the session.
User logout because of no authentication response from user.	The router logged off a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged off a user whose idle timeout period expired.
User logout because of user request.	A user logged off.
Local User Database does not support authentication mothed.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, check the RADIUS server.
Use Local User Database to authenticate user.	The local user database operates as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server operates as the authentication server.

Table 138 IEEE 802.1X Logs

Log Message	Description
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Log Commands

Go to the command interpreter interface (the Command Interpreter Appendix explains how to access and use the commands).

Configuring what you want the Business Secure Router to log

Use the sys logs load command to load the log setting buffer that allows you to configure which logs the Business Secure Router is to record.

Use sys logs category followed by a log category and a parameter to decide what to record.

Table 139 Log categories and available settings

Log Categories	Available Parameters
access	0, 1, 2, 3
attack	0, 1, 2, 3
error	0, 1, 2, 3
ike	0, 1, 2, 3
ipsec	0, 1, 2, 3
javablocked	0, 1, 2, 3
mten	0, 1
upnp	0, 1
urlblocked	0, 1, 2, 3

Table 139 Log categories and available settings

Log Categories	Available Parameters
urlforward	0, 1
	Use 0 to record no logs for a selected category, 1 to record only logs a selected category, 2 to record only alerts for a selected category, and 3 to record both logs and alerts for a selected category.

Use the sys logs save command to store the settings in the Business Secure Router (you must do this in order to record logs).

Displaying Logs

Use the sys logs display command to show all of the logs in the Business Secure Router's log.

Use the sys logs category display command to show the log settings for all of the log categories.

Use the sys logs display [log category] command to show the logs in an individual Business Secure Router log category.

Use the sys logs clear command to erase all of the Business Secure Router's logs.

Log Command Example

This example shows how to set the Business Secure Router to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                destination           notes
    message
  0|11/11/2002 15:10:12 |172.22.3.80:137       |172.22.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  1|11/11/2002 15:10:12 |172.21.4.17:138       |172.21.255.255:138    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  2|11/11/2002 15:10:11 |172.17.2.1            |224.0.1.60            |ACCESS BLOCK
    Firewall default policy: IGMP(set:8)
  3|11/11/2002 15:10:11 |172.22.3.80:137       |172.22.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  4|11/11/2002 15:10:10 |192.168.10.1:520      |192.168.10.255:520    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  5|11/11/2002 15:10:10 |172.21.4.67:137       |172.21.255.255:137    |ACCESS
BLOCK
```

Index

Numbers

10/100 Mb/s Ethernet WAN 34
3DES 207
4-Port Switch 34

A

Action 179
Action for Matched Packets 182
ActiveX 199
Address Assignment 58, 60
Administrator Inactivity Timer 79
AES 207
AH 206
AH Protocol 206
Alert 179
Allocated Budget 126
Allow Through IPSec Tunnel 247
Allow Trigger Dial 118
Always On 126
Answer 129
Application-level Firewalls 156
Applications 41
AT Command Initial String 124
AT Command Strings 127, 129
AT Response Strings 129
ATDP 127
ATH 127
Attack Alert 192, 194
Attack Types 162
Authentication databases 313
Authentication Header 206
Authentication Type 124
Autonegotiating 10/100 Mb/s Ethernet LAN 34
Autosensing 10/100 Mb/s Ethernet LAN 34
Auxiliary 35

B

Backup 399
Bandwidth Class 298
Bandwidth Filter 298, 305
Bandwidth Management 297
Bandwidth Management Statistics 306
Bandwidth Manager Class Configuration 303
Bandwidth Manager Class Setup 301
Bandwidth Manager Monitor 308
Bandwidth Manager Summary 300
Blocking Time 193, 195
Branch Office 222
Branch Tunnel NAT Address Mapping Rule 232
Broadcast Dial Backup Route 126
Brute force Attack 161
Brute Force Password Guessing Protection 37
Budget 126
Bypass Triangle Route 179

C

Cable Modem 157
Call Back Delay 129

Call Control 129
Call Scheduling 37, 385
  Maximum Number of Schedule Sets 385
  Precedence 385
  Precedence Example 385
Called ID 129
Calling Line Identification 129
Central Network Management 38
CHAP 124
Check WAN IP Address 122
CLID 129
Client IKE Source Port Switching 257
Client Minimum Version 258
Client Termination 248, 255
Client Termination IP Pool 254
Configuration 394
Connection ID/Name 112
Content Filtering 37, 197
  Days and Times 197
  Restrict Web Features 197
Contivity Client 216
Contivity VPN Client 213
Contivity VPN Client Software 35, 248
conventions, text 29
Cookies 199
copyright 2
Custom Port 182
Custom Ports
  Creating/Editing 184

D

Data Terminal Ready 127
DDNS Type 82
Default 398
Default Policy Log 179
Default Server 140
Default Server IP Address 139
Denial of Service 157, 158, 192, 193
DES 207
Destination Address 174, 182
DHCP 52, 60, 81, 93, 94, 394
DHCP (Dynamic Host Configuration Protocol) 39
DHCP Server 97
Dial 129
Dial Backup 122
Dial Backup Port Speed 124
Dial Timeout 129
DNS 77, 355
DNS Server
  For VPN Host 77
DNS Servers 94
Domain Name 52, 60, 79, 138
DoS
  Basics 158
  Types 159
DoS (Denial of Service) 36
Drop 129
Drop DTR When Hang Up 129
Drop Timeout 129
DSL Modem 41
DTE 127
DTR 127
DTR Signal 127
Dynamic DNS 81
Dynamic DNS Service Provider 82
Dynamic DNS Support 38
Dynamic Host Configuration Protocol 93
DYNDNS Wildcard 81, 83

E

ECHO 138
Enable Wildcard 83

Encapsulating Security Payload 206
ESP 206
ESP Protocol 206
Ethernet 52, 53, 56
Ethernet Encapsulation 107

F

Factory LAN Defaults 94
Fail Tolerance 122
Failover Tuning 257
Features 33
Finger 138
Firewall 36
  Access Methods 171
  Address Type 183
  Alerts 191
  Connection Direction 174
  Creating/Editing Rules 180
  Custom Ports 184
  Enabling 171
  Firewall Vs. Filters 169
  Guidelines For Enhancing Security 168
  Introduction 157
  LAN to WAN Rules 175
  Policies 171
  Rule Checklist 173
  Rule Logic 173
  Rule Security Ramifications 173
  Services 188
  Types 155
  When To Use 170
Firmware Version 392
First DNS Server 80
FTP 81, 137, 138, 327, 350
FTP Restrictions 327
FTP Server 40
Full Feature 116
Full Network Management 40

G

General Setup 51, 78
Global 132
Global End IP 142, 145
Global Start IP 142, 144
Group Authentication 219
Group ID 219, 250
Group Password 219, 250

H

Half-Open Sessions 192
Hardware Setup 42
Host 84
Host Names 82
How SSH works 342
HTTP 138, 156, 158, 159
HTTPS 36, 329
HTTPS Example 332

I

ICMP Commands That Trigger Alerts 162
ICMP echo 161
ICMP Vulnerability 162
Idle Timeout 112, 126
IEEE 802.1x 36
IGMP 95, 117, 126
IGMP-V1 117
IGMP-v1 126
IGMP-V2 117
IGMP-v2 126
Illegal Commands 162
Initial Contact Payload 258
Inside 132
Inside Global Address 132
Inside Local Address 132

Internet Control Message Protocol (ICMP) 161
Internet Group Multicast Protocol 95, 117
IP Address 58, 59, 137, 394
IP Alias 38, 101
IP Multicast 38
  Internet Group Management Protocol (IGMP) 38
IP Pool Setup 93
IP Ports 159
IP Spoofing 159, 163
IP Static Route 150
IPSec VPN Capability 35, 36
ISAKMP Initial Contact Payload 258

J

Java 199

K

Key Fields For Configuring Rules 174

L

LAN IP Address 378, 381
LAN Setup 93, 105
LAN TCP/IP 94
LAN to WAN Rules 175
LAND 160, 161
Local 132
Local End IP 142, 144
Local Start IP 142, 144
Log 179
Logging 40
Logs 371

M

MAC Addresses 100
MAIN MENU 48
Management Information Base (MIB) 352
Many One-to-One 143, 144
Many to Many No Overload 135
Many to Many Overload 135
Many to One 135
Many-to-Many Ov 144
Many-to-Many Overload 143, 144
Many-to-On 144
Many-to-One 143
Maximum Incomplete High 195
Maximum Incomplete Low 195
Max-incomplete High 193
Max-incomplete Low 193, 195
MD5 207
Media Access Control 100
Metric 105, 116, 121, 124, 153
Multicast 95, 117, 126
Multicast Version 126
My Password 319, 325

N

Nailed-up Connection 112
NAT 57, 59, 116, 125, 137, 138, 139, 140
  Application 134
  Definitions 131
  How NAT Works 133
  Mapping Types 135
  Port Restricted Cone 133
  Restricted Cone 133
  What NAT does 132
NAT Traversal 257, 359, 360, 361
NetBIOS commands 162
NetBIOS over TCP/IP 117, 247
Network Address Translation 116, 125
Network Address Translation (NAT) 39
Network Management 138

NNTP 138
Nortel Firmware Version 392
Number of Retransmissions 257

O

Off Line 83
On Demand Client Tunnel 219
One Minute High 195
One Minute Low 194
One to One 135
One-Minute High 193
One-to-One 144
Outside 132

P

Packet Direction 179, 181
Packet Filtering 37, 169
Packet Filtering Firewalls 156
PAP 124
Password 44, 83, 319, 325
Password Management 259
PAT 144
Phone Number 124
Ping of Death 159
Point-to-Point Protocol over Ethernet 108
Point-to-Point Tunneling Protocol 54, 110, 138
POP3 138, 158, 159
Port Configuration 184
Port Forwarding 39
Port Restricted Cone NAT 133
PPPoE 37, 52, 56, 57
PPPoE Encapsulation 108
PPTP 52, 54, 138
PPTP Encapsulation 38, 110
Predefined NTP Time Server List 85
Preshared Key 216, 240
Primary Phone Number 124
Priority 124
Private 116, 153
Private IP Address 58
Proportional Bandwidth Allocation 298
Protocol/Port 378, 380
publications
  hard copy 30
  related 30

Q

Quick Start Guide 43

R

RADIUS 309
  Shared Secret Key 310
RADIUS Message Types 309
regulatory information 2
Remote Management and NAT 328
Remote Management Limitations 327
Reports 376
Reset 46
Reset Button 35
Response Strings 127
Restore 400
Restrict Web Features 199
Retransmissions 257
Retry Count 129
Retry Interval 129
RIP 94, 95, 125
RIP Direction 95, 117
RIP Version 94, 117, 125
RIP-1 94, 117, 125
RIP-2 94

RIP-2B 95, 117, 125
RIP-2M 95, 117, 125
Roadrunner Manager 113
RoadRunner Support 40
RoadRunner Toshiba 113
Root Class 301
Routing Information Protocol 94
RR- Service Type 112
RR-Telstra 113
Rule Summary 187
Rules 171, 175
  Checklist 173
  Creating Custom 171
  Key Fields 174
  LAN to WAN 175
  Logic 173
  Predefined Services 188
  Source and Destination Addresses 183

S

SA Monitor 244
Saving the State 163
Schedule Sets
  Duration 388
Second DNS Server 80
Secondary Phone Number 124
Secure FTP Using SSH Example 347
Secure Telnet Using SSH Example 345
Security Ramifications 173
Server 88, 135, 136, 143, 144
Server Auto Detect 83
Service 174
Service Type 112, 179, 184
Services 138
setup a schedule 387
SHA1 207
Single User Account 125, 144
SMTP 138
Smurf 161, 162
SNMP 39, 138, 351
  Get 353
  Manager 352
  MIBs 353
  Trap 353
SNMP (Simple Network Management Protocol) 39
Source & Destination Addresses 183
Source Address 174, 182
SSH 36, 341
SSH Implementation 343
Start Port 148
Stateful Inspection 36, 155, 156, 163, 164, 165
  Process 164
Static DHCP 100
Static Route 149, 150
SUA 137, 138, 140
SUA (Single User Account) 136
SUA Only 116
SUA Server 139
Subclass Layers 301
Subnet Mask 59, 183
SYN Flood 160, 161
SYN-ACK 160
Syslog 187
System DNS Servers 80
System General Setup 79
System Name 79
System Screens 77
System Timeout 328

T

TA 127
TCP Maximum Incomplete 193, 194, 195

TCP Security 166
TCP/IP 158, 159, 160, 348
Teardrop 159
technical publications 30
Telnet 348
Telnet Configuration 348
text conventions 29
TFTP Restrictions 327
Third DNS Server 80
Threshold Values 192
Time and Date 35
Time Setting 86
Time Warner 113
Traceroute 163
Tracing 40
trademarks 2
Traffic Redirect 39, 119, 120
Trigger Port Forwarding Process 145

U

UDP/ICMP Security 167
Universal Plug and Play 37
Universal Plug and Play (UPnP) 359, 361
Upgradeable Firmware 40
Uploading a Configuration File Via Console Port 46
UPnP 37
UPnP Examples 363
UPnP Port Mapping 362
Upper Layer Protocols 167
URL Keyword Blocking 199
User Profiles 315
Username 44

V

VPN 110
VPN Client Termination 248

W

WAN MAC 118
WAN Setup 60
WAN to LAN Rules 175
Web Proxy 199
Web Site Hits 378
WebGUI 43, 47, 157, 168, 174
Windows Networking 117, 247
Wizard Setup 51, 52, 58
WWW 330

X

Xmodem Upload 47